Cyber-Threat Report

Agosto 2020

TG Soft
Cyber Security Specialist
www.tgsoft.it

Agosto 2020

TG Soft
Cyber-Threat Report

Notizie di rilievo:

DuckRat: Operazione Paperino

Panorama delle minacce in Italia a agosto

Sommario:

Nel mese di agosto si è riscontrato un lieve calo degli attacchi informatici ed una leggera diminuzione del numero dei cluster di malware rispetto al mese di luglio.
Ad agosto Emotet ha continuato le sue campagne di malspam verso l'utenza italiana, balzando al primo posto nella classifica dei malware più diffusi in Italia.
Nella prima settimana di agosto abbiamo una diversificazione degli attacchi malware. Nelle settimane a cavallo di ferragosto la maggior parte delle infezioni derivano da Emotet.
Ursnif è stato poco attivo ad agosto, riscontrate nuove campagne a tema "INPS".
Non sono mancati i vari password stealer come AgentTesla, MassLogger e QakBot. Vi sono stati attacchi RDP che hanno veicolato i ransomware: Matrix, Phobos e LockBit.
Ad agosto è stato identificato un nuovo cybercriminale italiano con lo spyware DuckRat nell'operazione "Paperino".

C.R.A.M.
CENTRO RICERCHE ANTI-MALWARE

TG Soft
Cyber Security Specialist
www.tgsoft.it

TG Soft S.r.l.

Via Pitagora n. 11/B
35030 Rubàno (PD)
Italy

Tel.: +39 049.8977432
Fax: +39 049.8599020
Email: info@tgsoft.it

Proteggiamo il tuo business dai cyber-criminali

www.tgsoft.it

TG Soft Cyber Security Specialist è produttore della suite di sicurezza Anti-Virus denominata **Vir.IT eXplorer** e presente nel settore della sicurezza informatica dai primi anni '90.

Il **C.R.A.M.** acronimo di Centro Ricerche Anti-Malware di TG Soft ha come obiettivi:

- PROMUOVERE e DIFFONDERE nel nostro Paese la cultura e la consapevolezza della Sicurezza Informatica in tutti i suoi aspetti.
- SUGGERIRE e PROPORRE atteggiamenti consapevoli e coerenti sulla Sicurezza Informatica e in particolare comportamenti da tenere, sia da parte degli utenti sia da parte dei consulenti informatici, per evitare di essere colpiti da virus/malware informatici;
- PROMUOVERE, ISTITUIRE e FAVORIRE iniziative per la formazione e la sensibilizzazione su vari temi della Sicurezza Informatica, in particolare tramite l'organizzazione di seminari e la pubblicazione di documenti e articoli relativi alla Sicurezza Informatica.

Seguici nei social:

Cyber-Threat Intelligence e Infection Rate

Al giorno d'oggi sono sempre più frequenti gli attacchi Cyber perpetrati contro le aziende. TG Soft analizza e cataloga queste minacce rilasciando report settimanali e mensili, dove vengono illustrati i trend del momento.

Il C.R.A.M. (Centro Ricerche Anti-Malware) di TG Soft raccoglie i dati della telemetria inviati dal software anti-virus Vir.IT eXplorer installato sui propri utenti/clienti e le informazioni di investigazione sui casi di attacchi informatici, per avere un quadro aggiornato della Cyber-Security in Italia.

L'indice che misura lo stato della Cyber-Security è l'Infection Rate (IR), che è la percentuale degli utenti dell'anti-virus Vir.IT eXplorer che hanno incontrato una minaccia che sia stata segnalata al C.R.A.M. di TG Soft.

L'Infection Rate può essere calcolato su un sotto-insieme di dati, ad esempio su un determinato sistema operativo, fornendo informazioni su quale possa essere il sistema operativo da considerarsi più sicuro. Le informazioni raccolte e analizzate ci permettono di determinare la tipologia degli attacchi, la frequenza con cui avvengono, la loro distribuzione e evoluzione nel breve e lungo periodo.

"Infection Rate: è la percentuale degli utenti che hanno incontrato almeno una minaccia segnalata al C.R.A.M. di TG Soft"

In primo piano

DuckRat: Operazione Paperino

Nel mese di agosto analizzando il caso di infezione di un nostro cliente, abbiamo scoperto una nuova tipologia di RAT (Remote Access Trojan), realizzata da un cyber-criminale italiano.

Questa tipologia di malware è stata denominata **DuckRat** in base al nome "**Paperino Project**" assegnatogli dal suo presunto autore.

Il vettore di diffusione utilizzato da DuckRat rimane sconosciuto, anche se ipotizziamo la compromissione di siti web.

DuckRAT è composto dai seguenti script e file eseguibili:

Nome file	Descrizione
Windows Update.vbs	Scarica i file **counter.vbs**, **HighPerformance.vbs** e **scheduler.vbs**. Esegue **WindowsLoader10.vbs**
WindowsLoader10.vbs	Esegue i file scaricati da **Windows Update.vbs**
Scheduler.vbs	Esegue lo script **win32.vbs**, che a sua volta esegue **win32.bat**
Win32.bat	Scarica i file **WindowsUpdater.vbs**, **load.exe**, **nircmd.exe**, **scr.vbs** e se stesso. Esegue il file **load.exe, nircmd.exe** e lo script **scr.vbs**

Load.exe

Il file Load.exe (md5 e94bea99baf305446401192631ea5c97) è un archivio autoestraente di WinRar protetto da password. La data di compilazione del file Load.exe è il 31 maggio 2020.

Al suo interno sono contenuti i seguenti file:

- WinRAR32.exe
- win32.exe

Il file **WinRAR32.exe** contiene il malware **DarkTrack Rat** , all'interno è presente la seguente configurazione:

- I_AM_DTVeKlSndv
- deansjuabsghansjk.ddns[.]net -> 5.89.123.231
- lusnuujajansussa.ddns[.]net -> 93.146.32.161

Le informazioni esfiltrate dal Rat vengono inviate ai server C2 presenti nella lista di configurazione.

Inoltre è presente la stringa "**Spanato**" che possiamo collegare all'autore di DuckRat.

Gli indirizzi IP assegnati dinamicamente ai server C2 utilizzati, sono stati geolocalizzati in Italia.

IP: 93.146.32.161

Counrty Code: IT
Counrty Name: Italy
Città: Seregno
Latitudine: 45.6563 **Longitudine:** 9.2116
ISP: Vodafone Italia DSL
ASN: AS30722 Vodafone Italia S.p.A.
Tipologia: residential

IP: 5.89.123.231

Counrty Code: IT
Counrty Name: Italy
Città: Naples
Latitudine: 40.8522 **Longitudine:** 14.2681
ISP: Vodafone Italia DSL
ASN: AS30722 Vodafone Italia S.p.A.
Tipologia: residential

Il file **Win32.exe** (md5 c76fc7fce3c4d15221036ac5d8929580) esegue i seguenti programmi della NirSoft:

- mpv.exe (Mail PassView)
- WBP.exe (WebBrowserPassView)
- mespv.exe (Instant Messengers Password Recovery)
- pv.exe (ProduKey)

Le informazioni esfiltrate attraverso i tool di NirSoft sono inviate al server ftp.drivehq[.]com attraverso le credenziali di accesso dell'utente "**donatopizza**".

E' stato individuato un'altra variante di Load.exe (con data di compilazione del 25 giugno 2020), che includeva una versione di WinRAR32.exe infetto dal Rat **Fynloski** (**DarkComet**).

Nircmd.exe & scr.vbs

Dopo che **Win32.bat** ha eseguito il file **load.exe**, viene mandato in esecuzione il tool **Nircmd.exe** della NirSoft con il seguente comando:

```
nircmd.exe savescreenshotfull "%computername% ~$currdate.dd_MM_yyyy$
~$currtime.HH.mm$ .png"
```

dove viene catturato lo schermo del computer e salvato in un'immagine png.

A questo punto viene eseguito lo script **scr.vbs**, che invia un email con allegato l'immagine png appena catturata:

- Mittente: **pinoilcamionista@gmail.com**
- Destinatario: **paperinoproject@protonmail.com**
- Oggetto: TestCDO

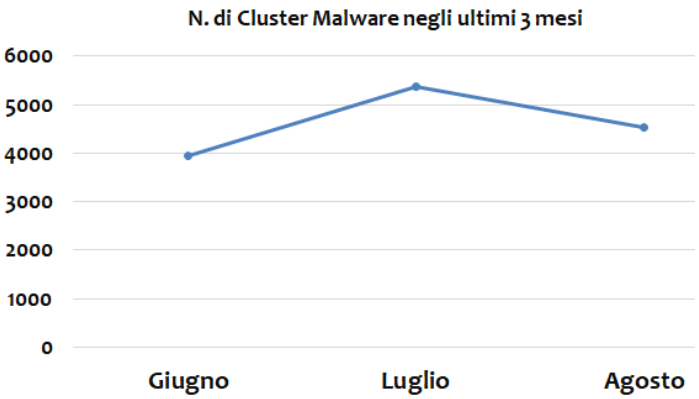
Questa operazione di "catturare lo schermo" viene ripetuta ogni 10 minuti attraverso la schedulazione degli script del malware.

L'arsenale di DuckRat è costituito dai RAT "DarkTrack" e "Fynloski", per l'esfiltrazione di dati (file e password) e controllo della macchina della vittima, da numerosi altri tool della NirSoft per il recupero di password dalle mail e memorizzate nel browser, nonché serial number dei software come Windows e Office. I primi riferimenti del cyber-criminale, dall'analisi dei file eseguibili, risalgono al 31 maggio 2020. Nuovi moduli contrassegnati con la data del 25 giugno 2020 e l'attacco di agosto ci portano a pensare che l'operazione "Paperino" sia ancora in corso. Il cyber-criminale di DuckRat si presume possa essere italiano, gli indirizzi IP dei server C2 sono stati geolocalizzati in Italia, gli indirizzi email e l'account utilizzato per esfiltrazione dei dati sono riferiti a nomi italiani, tutto questo fa presumere di essere di fronte ad un nuovo attore italiano.

Statistiche Malware

Agosto 2020—ITALIA

I dati della telemetria del C.R.A.M. di TG Soft sono raccolti dagli utenti che utilizzano il software antivirus Vir.IT eXplorer. Le segnalazioni derivano da attacchi bloccati oppure malware riscontrati all'interno del parco macchine monitorato. Ogni minaccia identificata da Vir.IT viene classificata in famiglie e in cluster di malware. Ogni cluster di malware può contenere uno o più samples, ad esempio **Office.VBA.Macro_Heur** può identificare centinaia o migliaia di macro virus distinti.

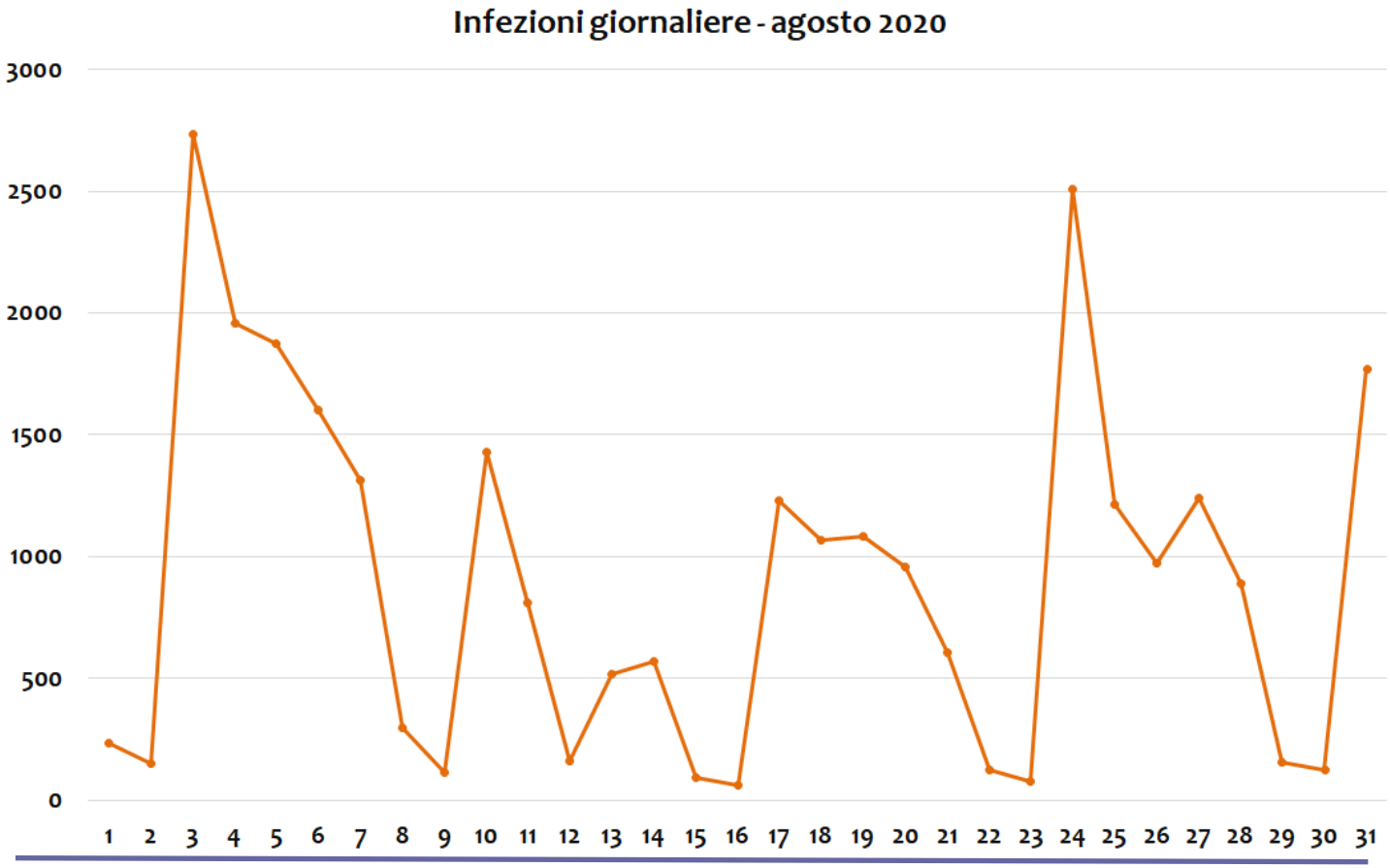


Nel mese di agosto abbiamo avuto una flessione del numero di malware rispetto al precedente mese di luglio, dove erano stati riscontrati 5364 cluster di malware contro i 4527 del mese di agosto. Questo decremento può essere dovuto alla chiusura estiva di molte aziende italiane.

Nel grafico a fondo pagina possiamo vedere l'andamento giornaliero delle infezioni in Italia.

All'inizio del mese, lunedì 3 agosto, abbiamo avuto un picco di segnalazioni d'infezione, dovute alle scansioni automatiche mensili del motore antivirus Vir.IT eXplorer. Nelle due settimane successive a cavallo di ferragosto, abbiamo un sensibile calo delle infezioni giornaliere, che oscillano in una fascia che va dalle 50 alle 1500 segnalazioni. Il punto minimo delle infezioni avviene nel weekend di ferragosto.

Nell'ultima settimana abbiamo una crescita delle infezioni, dovute alla ripresa di molte aziende dalla pausa estiva.



Nel grafico sottostante vediamo le statistiche relative al mese di agosto 2020 suddivise per "Tipologia Malware" riscontrate in Italia.

Con il termine malware intendiamo qualsiasi tipologia di software malevolo che possa arrecare danno al sistema informatico.

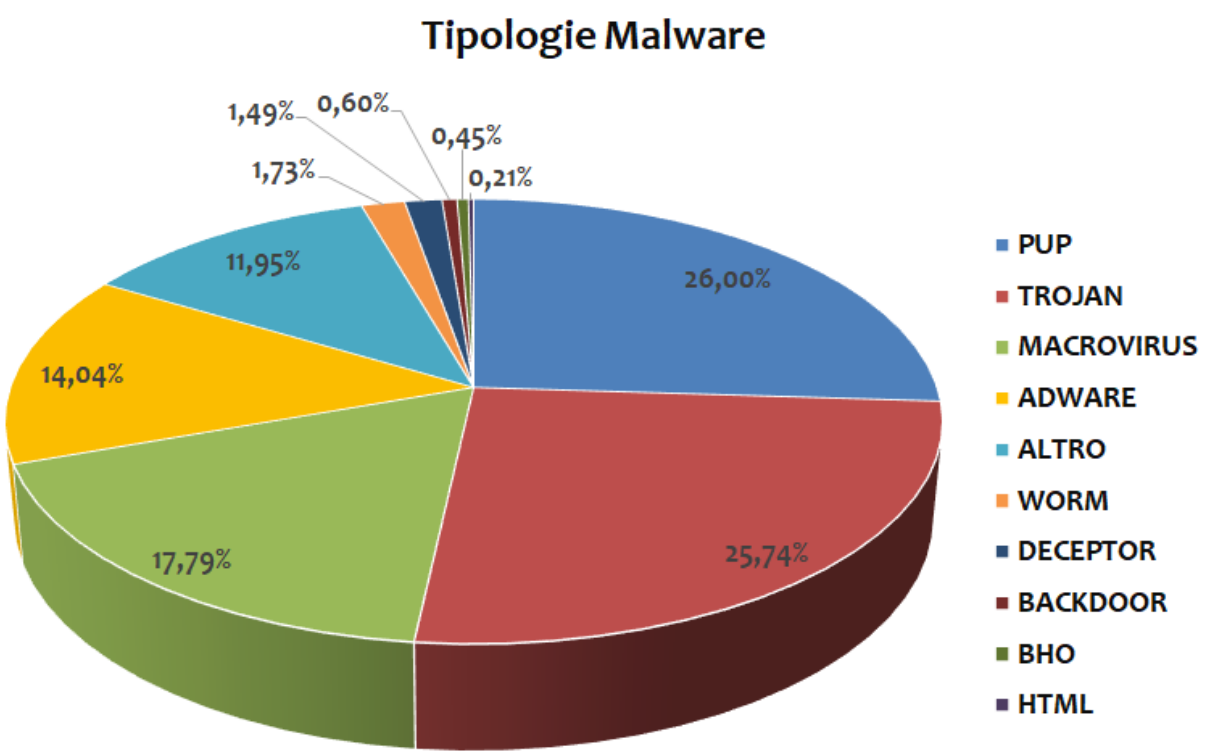
I malware si suddividono in diverse tipologie: Adware, Backdoor, Trojan, Worm, Virus, PUA/PUP, Deceptor, etc.

Nel mese di agosto la tipologia dei **PUP** si riconferma in prima posizione con il 26,00% delle infezioni in leggero calo rispetto a luglio. Al secondo posto troviamo i **TROJAN** con il 25,74%, stabili rispetto a luglio. Al terzo posto troviamo la famiglia dei **MACROVIRUS** con il 17,79%, in leggero aumento rispetto al mese scorso. Gli **ADWARE** si mantengono al quarto posto con un 14,04% anche se in calo di un punto percentuale.

E' interessante notare che le prime 4 tipologie di malware rappresentano l'84% delle infezioni monitorate.

Al quinto posto troviamo il gruppo denominato **ALTRO**, che include i virus, con l'11,95% delle infezioni in leggera crescita rispetto a luglio. In sesta posizione troviamo i **WORM** con l'1,73% che guadagnano due posizioni rispetto a luglio, seguono i **DECEPTOR** con l'1,49% e chiudono la classifica le **BACKDOOR,** i **BHO** e gli **HTML.**

MACROVIRUS: sono costituiti dalle macro malevoli di Office e di altri software, che possono scaricare altri malware. Negli anni '90 erano catalogati come virus, perché potevano diffondersi



Analizziamo le statistiche di agosto dei singoli Malware. Questo mese balza al primo posto l'**Office.VBA_Macro_Heur** (tipologia MACRO VIRUS) , con un'imponente 9,12% delle infezioni, un incremento di 3 punti percentuali rispetto a luglio.

Si tratta di un dato ottenuto tramite l'analisi euristica e riguardano i file contenenti macro potenzialmente pericolose ed includono i documenti infettati da **Emotet**.

Al secondo posto troviamo il de-troneggiato **PUP.Win32.MindSpark** con la solita variante "F" con il 5.43% delle infezioni, che può compromettere il tuo browser, modificando l'home page e il motore di ricerca.

Al terzo posto troviamo una vecchia conoscenza il virus **Win32.Tenga.A** con il 2,16% delle infezioni. Il virus Tenga si propaga infettando i file eseguibili, il vettore di infezione potrebbe essere legato all'aggiornamento di qualche gestionale.

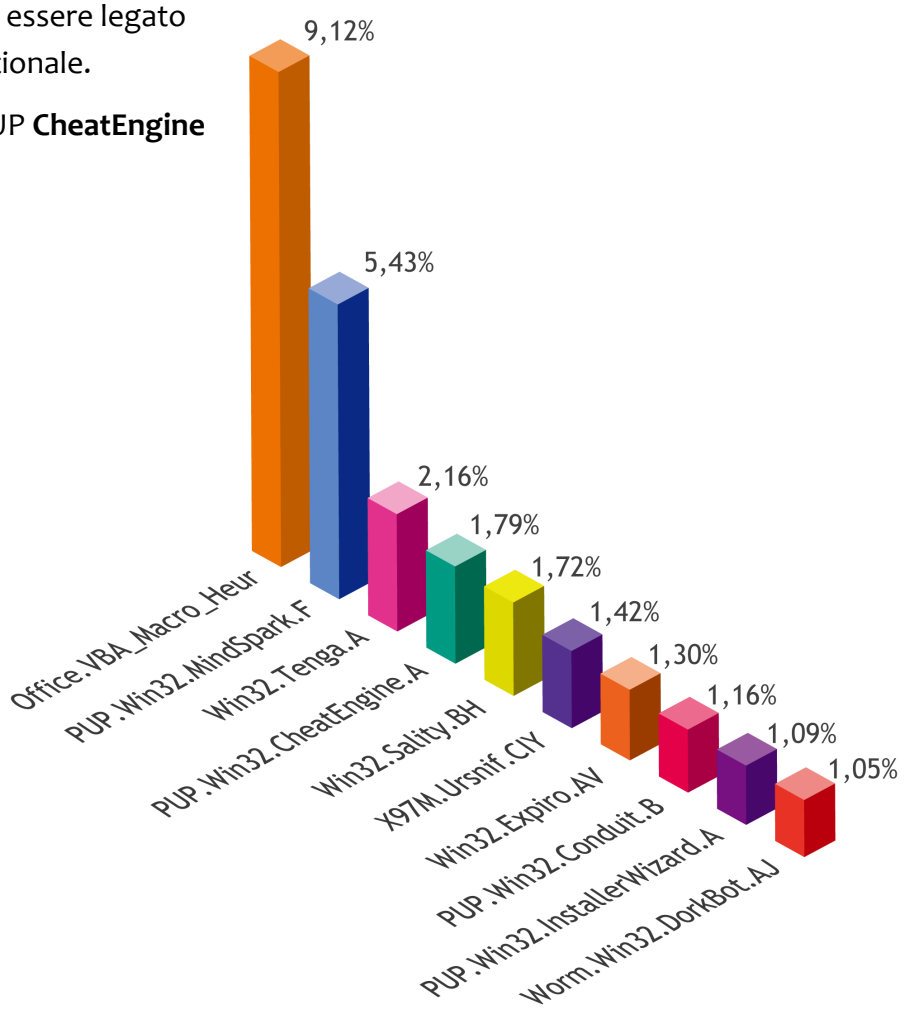
In quarta posizione troviamo il PUP **CheatEngine** con l'1,79% delle infezioni rilevate.

I malware della Top10 rappresentano il 26,24% delle infezioni di agosto, il rimanente 73,76% è dato da altri 4517 cluster di malware.

Anche questo mese nella Top10 troviamo due vecchie conoscenze del mondo dei virus, sono il virus polimorfico **Win32.Sality.BH** (in quinta posizione) e il **Win32.Expiro.AV** in settima posizione.

Nella Top10 non poteva mancare il trojan bancario **Ursnif** che si piazza in sesta posizione, attraverso le infezioni rilevate nei fogli elettronici di Excel e classificate con il nome di **X97M.Ursnif.CIY**.

I malware della Top10 rappresentano il 26,24% delle infezioni del mese di agosto, il rimanente **73,76%** è dato da altri 4517 cluster di malware.

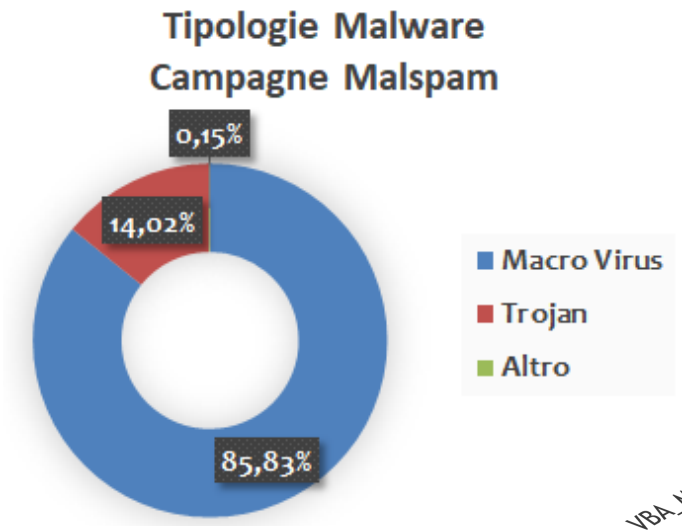


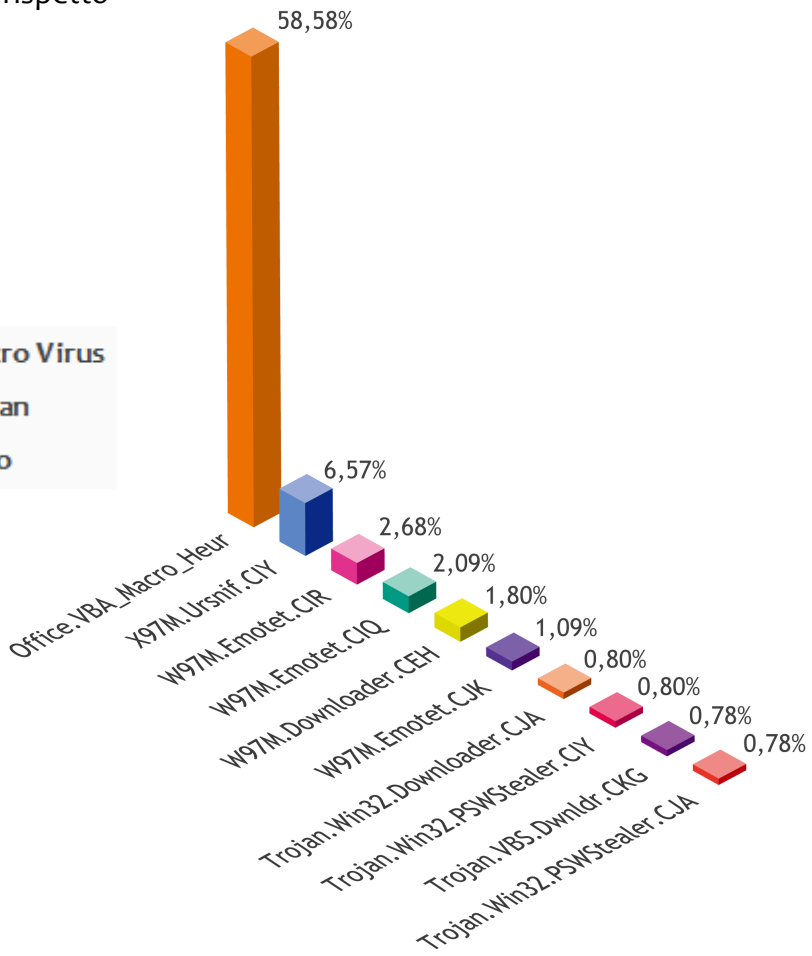
Statistiche Malware via email

Agosto 2020—ITALIA

Analizziamo ora le campagne di malware veicolate via email nel mese di agosto. Anche in questo caso possiamo suddividere le statistiche per tipologia e singolo malware.

La categoria dei **MACRO VIRUS** mantiene sempre la prima posizione con il 85,83% (+6,01%). Il dato ottenuto, segna un notevole incremento rispetto a luglio grazie alle massive campagne di malspam di Emotet. Seguono la tipologia dei **TROJAN** che con il 14,02% (-5,87%) si confermano al secondo posto. Al terzo posto troviamo la tipologia **ALTRO** con lo 0,15% che include varie tipologie come **WORM** e **BACKDOOR**.





Analizzando le statistiche delle campagne di malspam per singolo malware, al primo posto troviamo l'**Office.VBA_Macro_EUR** (tipologia Macro Virus) , che include il malware **Emotet** con il 58,58%. Al secondo posto troviamo il trojan bancario chiamato **Ursnif**, staccato di oltre 50 punti percentuali dalla prima posizione. Le varianti di **X97M.Ursnif** presenti nella Top10 questo mese sono solo una, erano 6 a luglio. In terza, quarta e sesta posizione troviamo altre tre varianti di Emotet. Sempre appartenente alla tipologia dei MACRO VIRUS, troviamo il **W97M.Downloader.CEH** con l'1,80%.

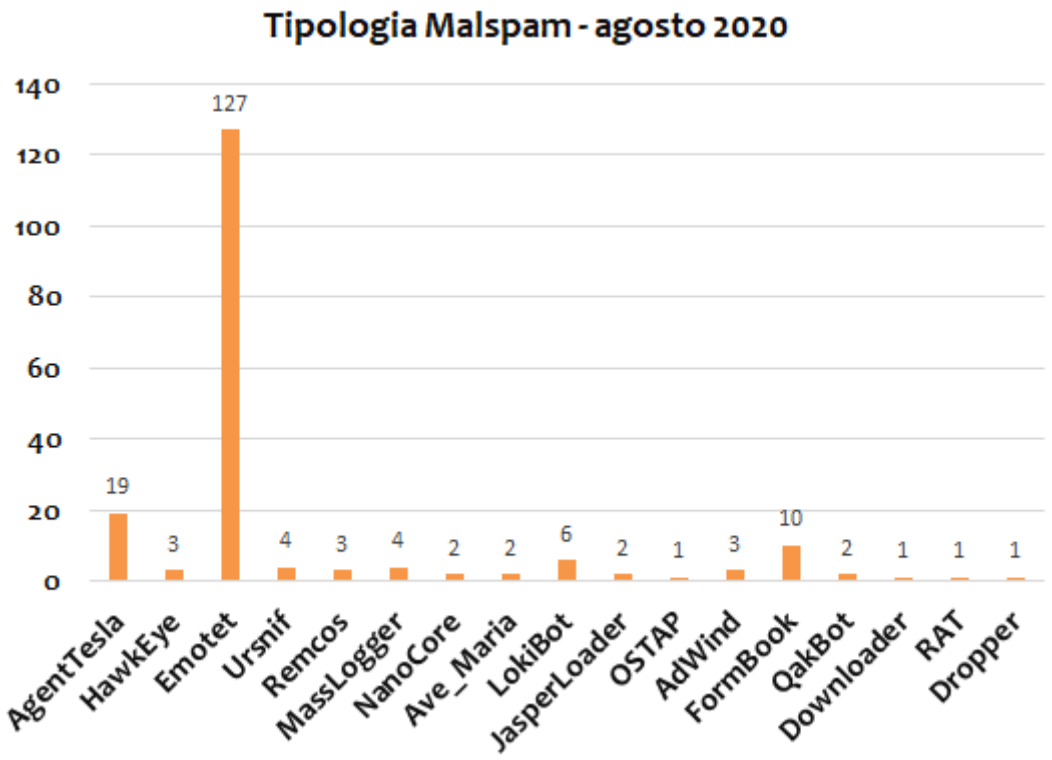
Nelle prime 6 posizioni della Top10 delle mail, troviamo esclusivamente MACRO VIRUS, che rappresentano il 72,81% delle infezioni di agosto, il rimanente 27,19% è dato da altri 477 malware.

Come era prevedibile ad agosto Emotet ha staccato la concorrenza attraverso massive campagne di malspam in tutto il mondo.

Analisi dei malware di agosto

Nel mese di agosto in Italia, attraverso le campagne di malspam che hanno "targettizzato" l'utenza italiana (email scritte in lingua italiana), sono stati veicolati 17 differenti tipologie di malware.

Nella figura sottostante possiamo vedere l'andamento dei malware distribuiti attraverso il vettore d'infezione della posta elettronica nel mese di agosto.



Ad agosto **Emotet** non si è preso una pausa, con le sue 127 campagne di malspam contro l'utenza italiana si aggiudica la prima posizione. Emotet è un trojan downloader che può scaricare altri malware nel computer della vittima.

AgentTesla, un password stealer che ruba le credenziali di accesso, risulta essere molto utilizzato da diversi attori cyber-criminali ad agosto.

In terza posizione troviamo **FormBook** con 10 campagne di malspam, seguito da **LokiBot** con 6 campagne. Invece il trojan banker **Ursnif** rallenta ad agosto con solo 4 campagne di malspam. Lo scopo di questo malware è di rubare le credenziali di accesso all'home banking per svuotare il conto corrente.

Nel mese di agosto sono stati monitorati altri password stealer o rat come:

- HawkEye
- Remcos
- MassLogger
- NanoCore
- Ave_Maria
- AdWind

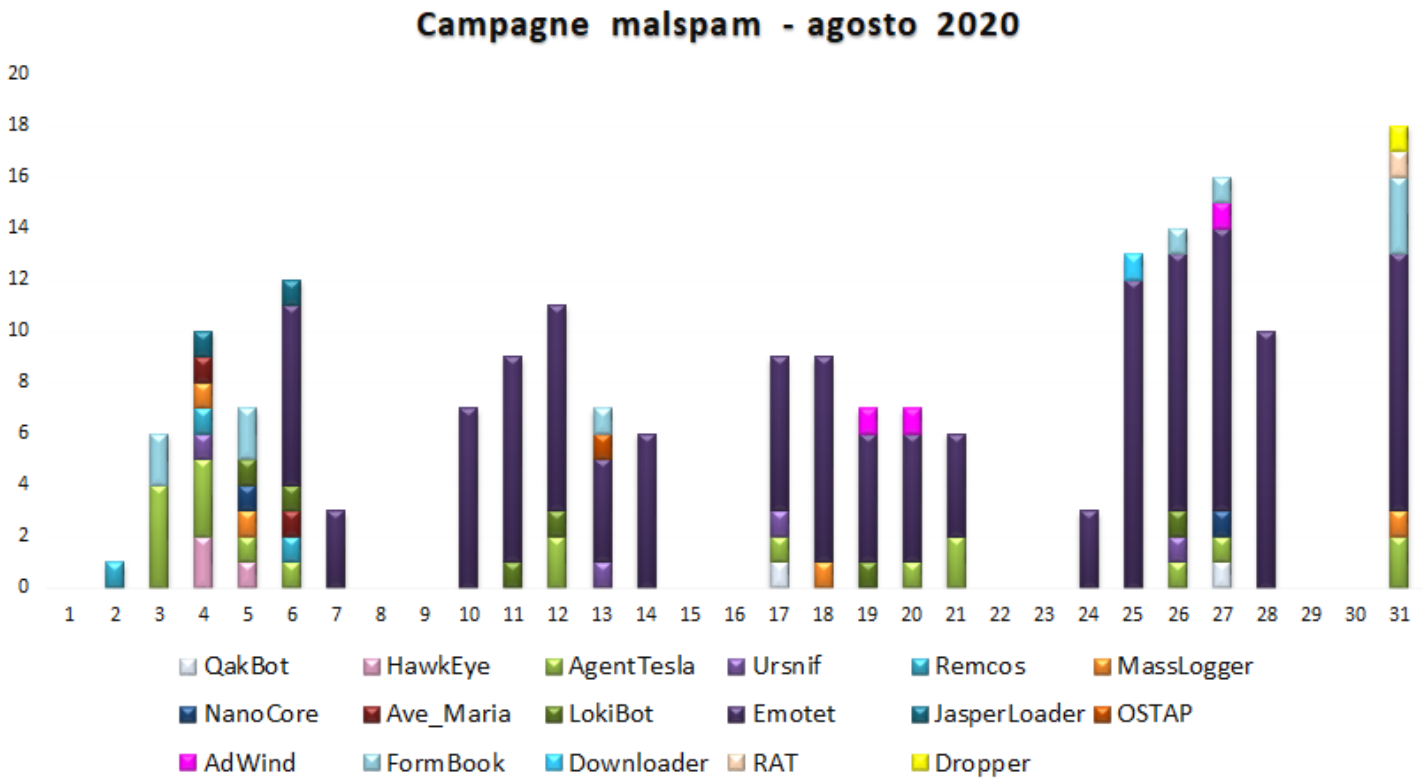
Tutti queste tipologie di malware hanno lo scopo di rubare le password, le informazioni riservate dal computer della vittima o spiarlo.

Sono continuate le campagne di malspam di **JasperLoader** nella prima settimana di agosto.

Due new entry di agosto sono il trojan **QakBot** e **OSTAP**. Continuano gli attacchi di **Hagga** ad agosto.

Nella figura sottostante possiamo vedere l'andamento giornaliero delle campagne di malspam con target Italia.

Nel mese di agosto Emotet ha iniziato a "spammare" da giovedì 6 e nei primi giorni non abbiamo monitorato sue campagne. Se escludiamo Emotet, nella prima settimana di agosto abbiamo una diversificazione di malware. Invece nelle settimane centrali a cavallo di ferragosto si è notata una forte diminuzione delle campagne di malspam atte a veicolare altri malware, dovute sicuramente alla chiusura estiva delle aziende italiane. Emotet sta "soffocando" le campagne di malspam degli altri malware.



E' possibile consultare le campagne di malspam settimanali del mese di agosto dai seguenti link:

Week 31 ==> dall'1 al 7 agosto

Week 32 ==> dall'8 al 14 agosto

Week 33 ==> dal 15 al 21 agosto

Week 34 ==> dal 22 al 28 agosto

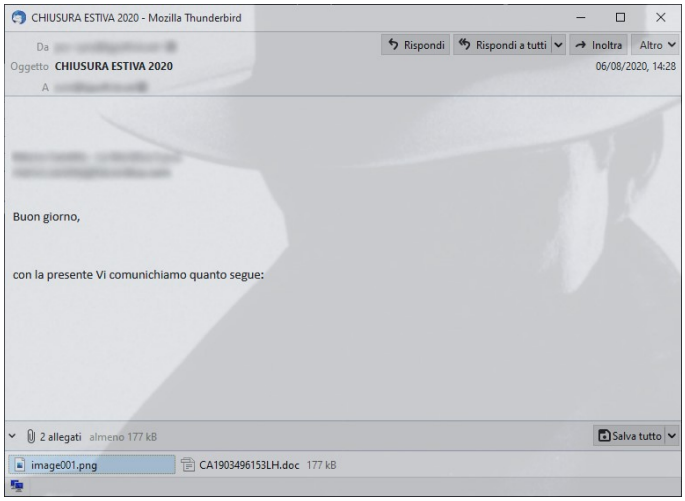
Week 35 ==> dal 29 agosto al 4 settembre

Emotet

Analisi delle campagne di agosto

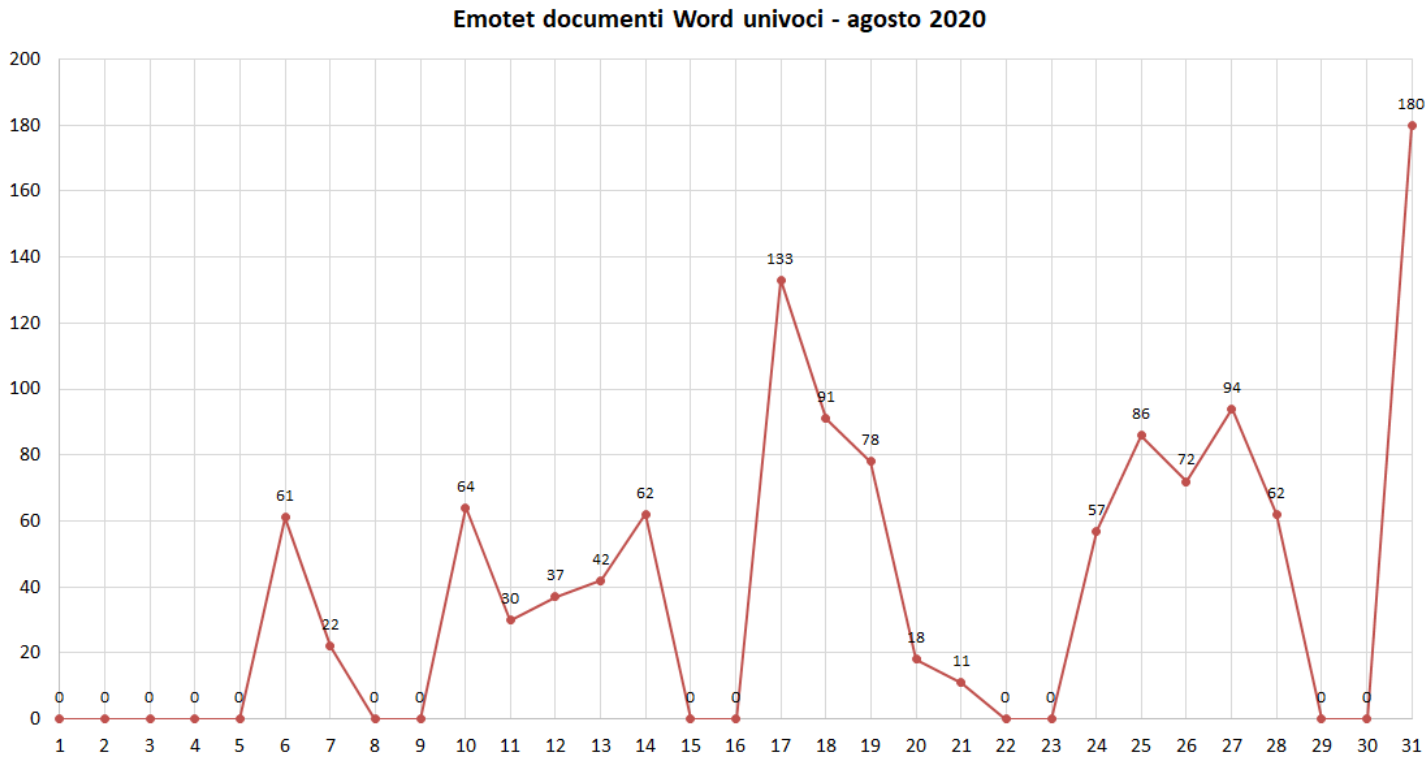
Nel mese di agosto **Emotet** non è andato in vacanza e ha veicolato numerose campagne di malspam.

Nell'immagine a destra vediamo un esempio di email del 6 agosto con allegato un documento di Word infetto da Emotet.



Ad agosto nei primi cinque giorni Emotet non ha "spammato", da giovedì 6 agosto ha ripreso con le sue massive campagne di malspam. Molto probabilmente l'attore di Emotet, denominato con il nome di "Ivan", in quei giorni stava lavorando per migliorare la propria infrastruttura.

Nella figura sottostante possiamo vedere l'andamento giornaliero dei documenti di Word univoci infetti da Emotet distribuiti via email nel mese di agosto in Italia. Come possiamo vedere dal grafico, il numero di documenti distinti allegati alle campagne di malspam di Emotet, registra il suo picco massimo (con 180 hash univoci) lunedì 31 agosto, giorno in cui la maggior parte delle aziende italiane ha ripreso a lavorare dopo la chiusura estiva. Emotet è in grado di inviare da ogni computer infetto (appartenente alla botnet) un'elevata quantità di malspam (superiore alle 50000 mail/giorno) , rubando gli oggetti e i corpi dei messaggi originali dalle mail delle vittime già compromesse. Le mail infette, che contengono in allegato un documento di Word con Emotet, vengono inviate come risposta ai destinatari delle email rubate.



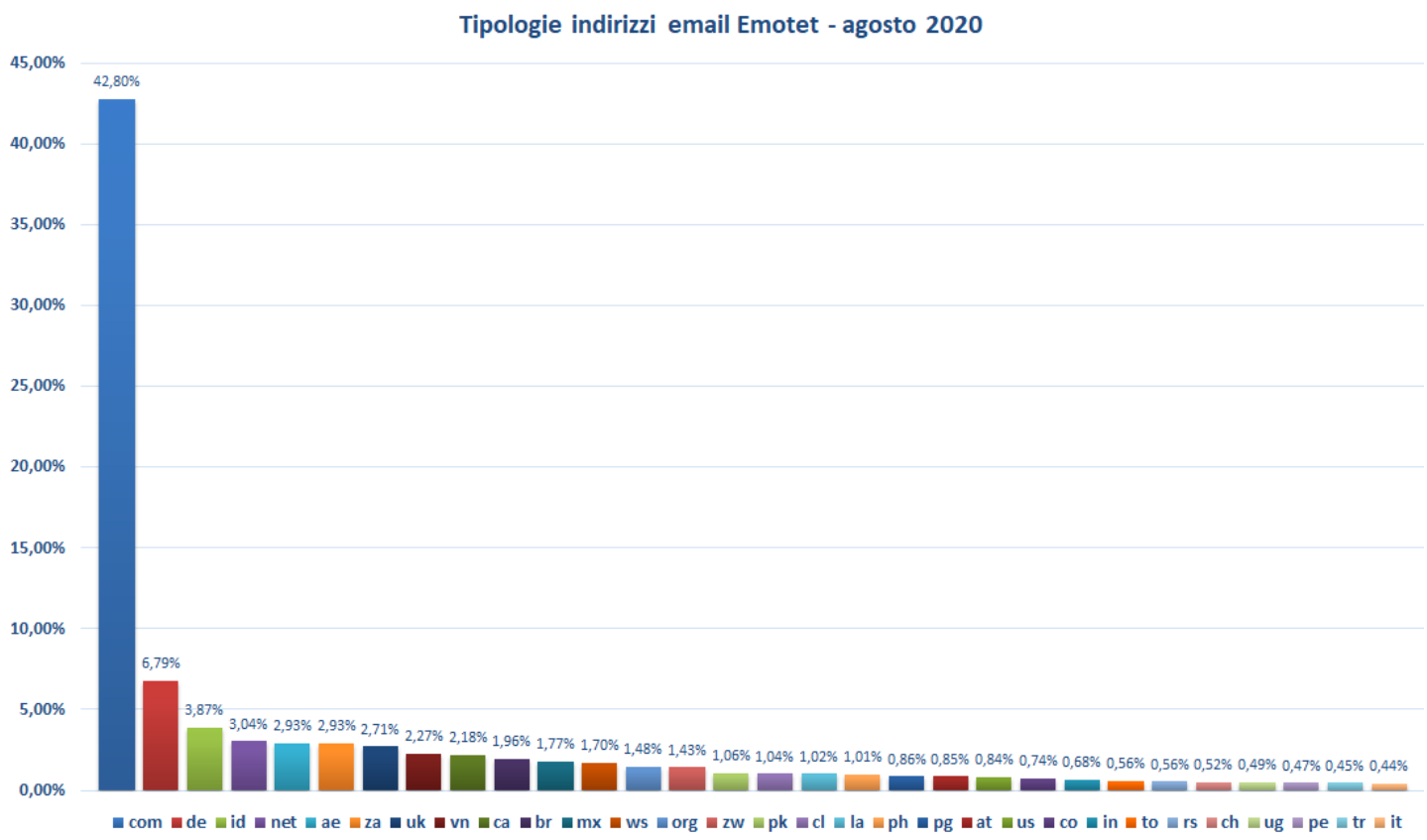
Questa tecnica di rispondere alle email rubate, falsificando il mittente originale, inganna il destinatario del messaggio che, in buona fede, procedendo ad aprirlo, si infetterà. Questa tecnica è stata utilizzata in passato dal malware Ursnif.

Emotet è un malware molto pericoloso, perché è in grado di infettare la rete aziendale utilizzando la tecnica dello "spostamento laterale", oppure attraverso un approccio indiretto rispondendo ad email interne tra colleghi della stessa azienda.

Nel grafico sottostante possiamo vedere la tipologia degli indirizzi email (Top Level Domain) a cui è stato "spammato" Emotet. In questa particolare rappresentazione, sono state prese come campione di analisi più di 277.000 email monitorate dal C.R.A.M. nel mese di agosto.

Al primo posto troviamo con oltre il 42% dei messaggi inviati gli indirizzi email "**.com**". Gli indirizzi email ".com" sono di tipo "commerciale" e non sono assegnati ad un Paese specifico. Al secondo posto troviamo con il 6.79% gli indirizzi email "**.de**" della **Germania**. L'**Indonesia** si posiziona al terzo posto con il 3,87% . Gli **Emirati Arabi** (ae) si posizionano al quinto posto, davanti al **Sud Africa** (za), **Gran Bretagna** (uk), **Vietnam** (vn), **Canada** (ca) e **Brasile** (br).

L'**Italia** si posiziona al 31-esimo posto con lo 0,44% delle email inviate verso indirizzi "**.it**".

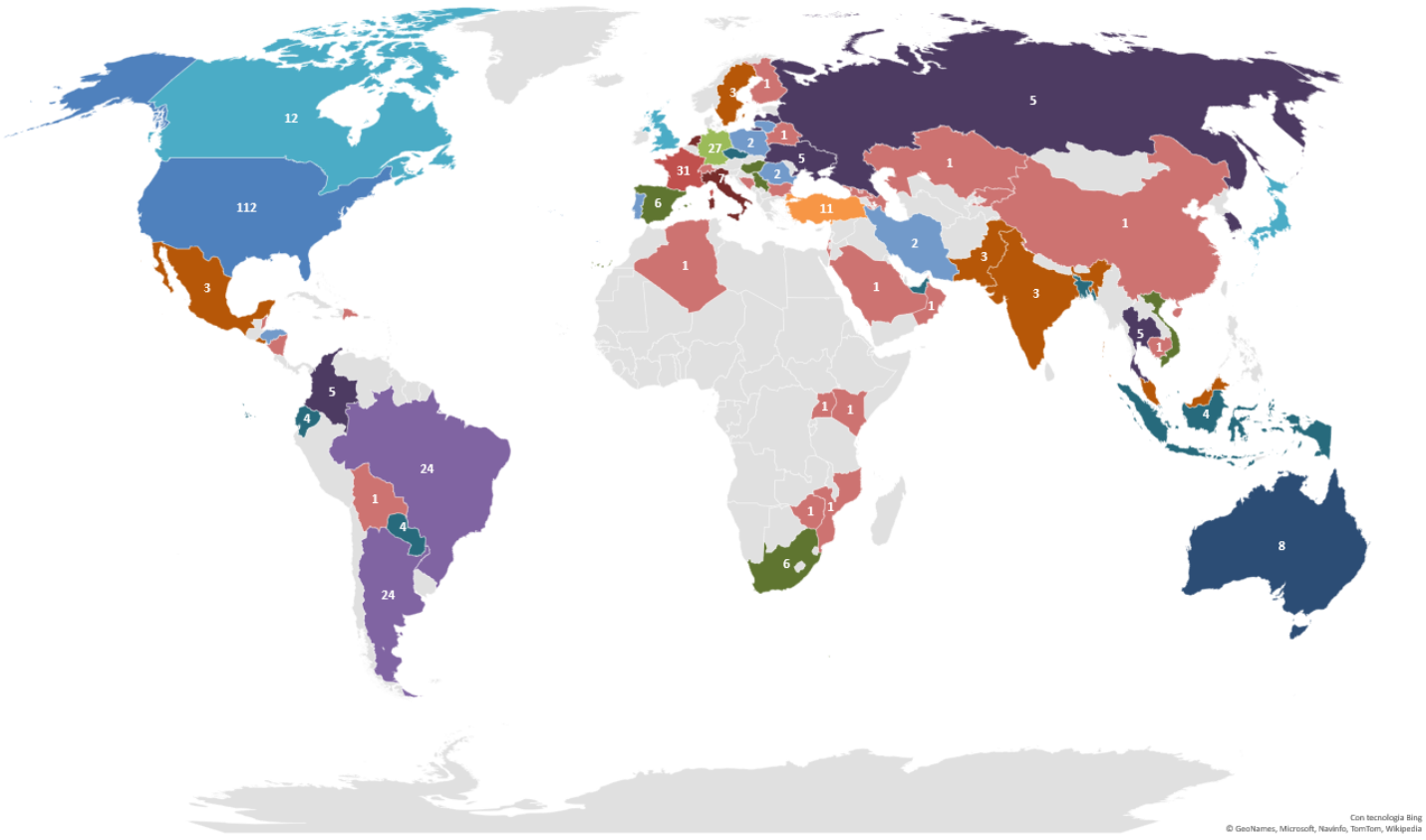


Le informazioni rubate dai computer delle vittime vengono inviate ad una serie di server di comando e controllo dell'Emotet. Questi computer che hanno la funzione di server C&C sono distribuiti in tutto il mondo.

Nella mappa sottostante possiamo vedere la geo-localizzazione dei server di comando e controllo di Emotet utilizzati nel mese di agosto.

Ad agosto Emotet si è collegato a più di **440 server C&C**. La maggior parte di questi si trovano negli **Stati Uniti d'America (112 server),** come possiamo vedere nella tabella a fianco. Al secondo e terzo posto troviamo rispettivamente Francia e Germania. L'**Italia** si posiziona al decimo posto con **7 server** di comando e controllo.

Stato	Num. Server C2
Stati Uniti	112
Francia	31
Germania	27
Argentina	24
Brasile	24
Giappone	12
Gran Bretagna	12
Turchia	11
Australia	8
Italia	**7**
Olanda	7
Ungheria	6
Serbia	6
Spagna	6
Sud Africa	6
Vietnam	6
Altri Paesi	135



In Italia vi sono 7 server di comando e controllo, come possiamo vedere dalla seguente tabella:

IP	Città	Provider
2.47.112.152	Napoli	Vodafone Italia S.p.A.
93.151.186.85	Gravina In Puglia	Vodafone Italia S.p.A.
91.231.166.124	Vitulazio	Libra S.r.l.
93.51.50.171	Aversa	Fastweb
109.116.214.124	Palermo	Vodafone Italia S.p.A.
89.186.91.200	Padova	Irideos S.p.A.
93.147.212.206	Castellammare Del Golfo	Vodafone Italia S.p.A.

Il Trojan Emotet scarica come follow-up il malware **QakBot** e **TrickBot**. Nell'attacco dell'anno scorso (settembre 2019 — febbraio 2020) scaricava solamente il malware **TrickBot,** che a sua volta scaricava il ransomware **Ryuk.**

Ursnif

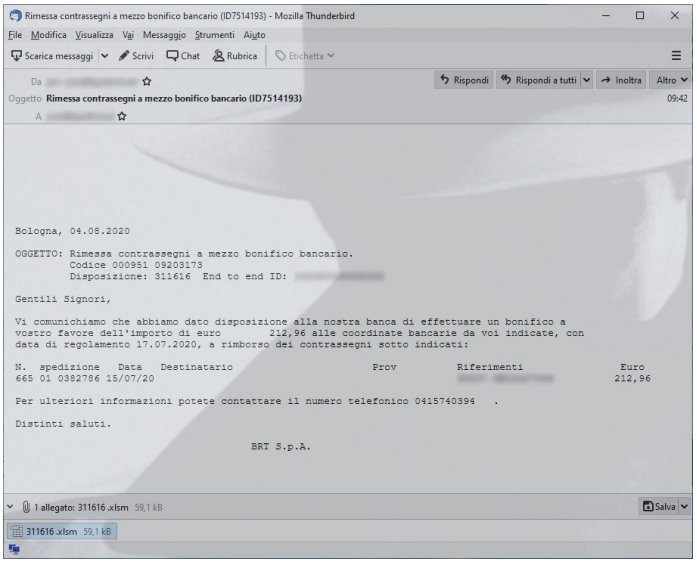
Analisi delle campagne di agosto

Analizziamo ora le campagne del malware bancario **Ursnif** (noto anche come **Gozi** o **IFSB**) nel mese di agosto.

Come abbiamo visto, questo malware è uno dei più diffusi via email in Italia, ma ad agosto è stato veicolato solamente attraverso 4 campagne di malspam.

Come si può vedere dalla figura a fianco, l'andamento delle campagne ne ha risentito ad agosto, molto probabilmente dovuto al fatto che la maggior parte delle aziende italiane sono chiuse per ferie.

Abbiamo una prima campagna a tema "Bartolini" ad inizio mese, per poi avere nelle settimane successive tre campagne a tema "INPS".



Ursnif—Campagne Malspam

04/08/2020	Rimessa contrassegni BRT
13/08/2020	INPS
17/08/2020	INPS
26/08/2020	Naz. Previdenza Sociale

Ad agosto i cyber-criminali hanno usato il nuovo tema dell'INPS al posto dell'Agenzia delle Entrate.

Dall'analisi delle campagne di malspam e dalle configurazioni individuate all'interno del trojan bancario Ursnif utilizzato, vi sono due gruppi distinti che stanno sfruttando questo malware a agosto per attaccare l'utenza italiana.

Ad agosto è stato abbandonato il tema dell'Agenzia delle Entrate per utilizzare un nuovo filone relativo all'INPS.

Questi due gruppi cyber risultano essere attivi in Italia da diversi mesi. Il primo sfrutta temi istituzionali italiani, come ad esempio l'Agenzia delle Entrate oppure l'INPS come in questo mese. Il secondo invece sfrutta il tema di fatture o ordini collegati a società di spedizione come BRT (Bartolini) o DHL.

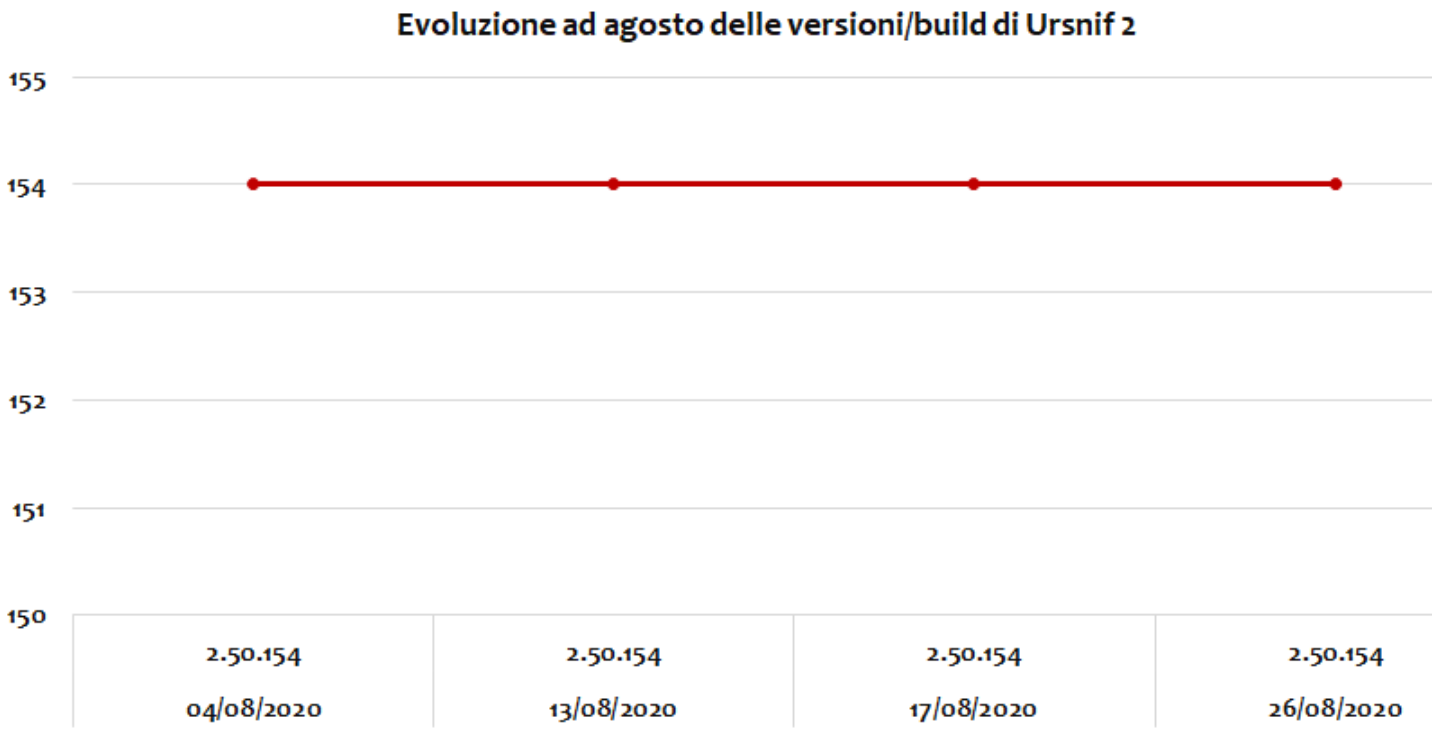
Ursnif è un trojan bancario, i cui sorgenti essendo divenuti di pubblico dominio, hanno originato un "fork", che ha portato allo sviluppo delle seguenti:

- Versione 2
- Versione 3

In Italia sono circolati, fino ad aprile, entrambe le versioni, ma nel mese di agosto è stata rilevata esclusivamente la versione 2.

Nel grafico sottostante possiamo vedere l'evoluzione dello sviluppo del trojan banker Ursnif utilizzato negli attacchi in Italia. Nell'ascissa abbiamo la data della campagna di malspam e la corrispondente versione utilizzata di Ursnif. Nell'ordinata abbiamo la build di sviluppo del malware Ursnif.

Nel mese di agosto non vi sono stati aggiornamenti nel malware Ursnif, la build utilizzata nelle varie campagne dai due gruppi è sempre stata la 154, si potrebbe pensare che gli autori di Ursnif in agosto si siano presi qualche giorno di vacanza.



Hagga

Analisi delle campagne di agosto

Nel mese di agosto il cyber-criminale denominato con il nome di **Hagga** ha diffuso nuove campagne di malspam con l'obiettivo di colpire l'utenza italiana. Hagga è un cyber-criminale attivo dal 2018 che ciclicamente attacca società italiane, ma non solo, vi sono campagne tedesche, inglesi e americane, per rubare password e/o credenziali di accesso, attraverso password stealer o rat commerciali.

Ad agosto sono state quattro le campagne di malspam diffuse in Italia:

- 6 agosto 2020
- 11 agosto 2020
- 12 agosto 2020
- 19 agosto 2020

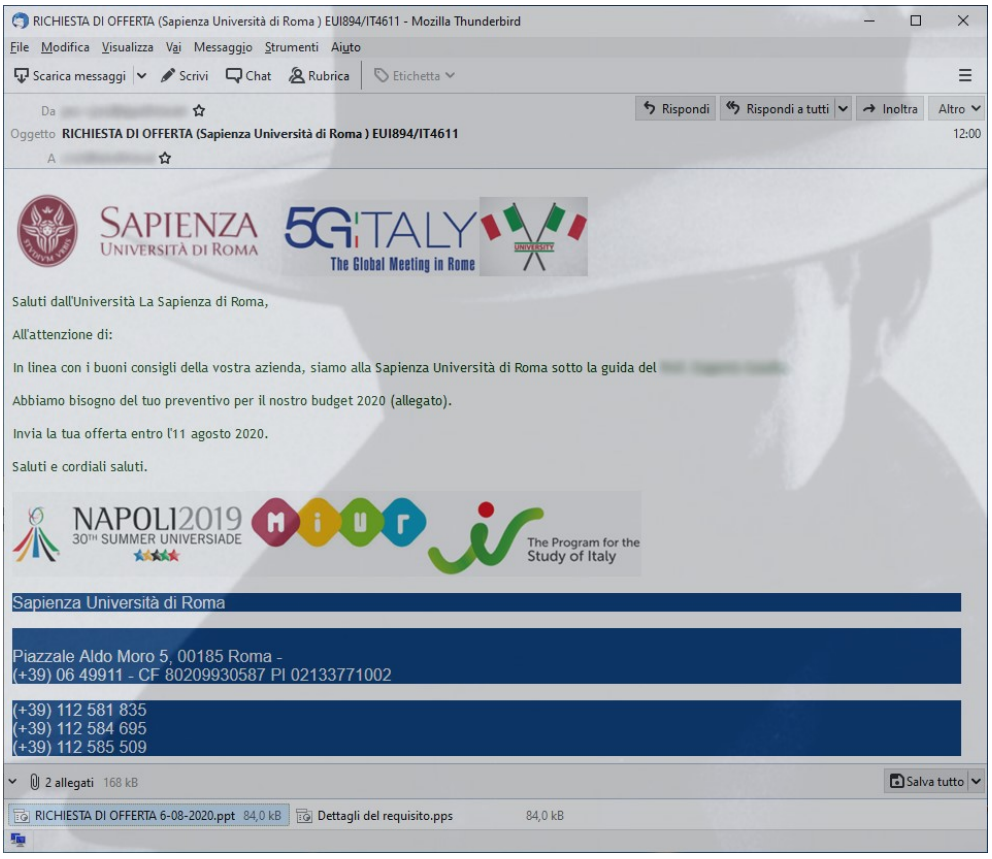
In tutti i casi il tema delle campagne utilizzate erano riferite ad una richiesta di offerta da parte dell'**Università della Sapienza** di Roma, come possiamo vedere nell'immagine sottostante dell'email del 6 agosto 2020.

In tre attacchi su quattro di agosto, documenti di PowerPoint infetti erano allegati all'email, con lo scopo di scaricare ed eseguire, dopo una serie di download di script memorizzati nel portale di *PasteBin,* il password stealer **LokiBot**. Solo in un caso l'allegato malevolo era direttamente un file eseguibile infetto con LokiBot.

L'identificativo Hagga deriva dal nome di un utente utilizzato su Pastebin in passato per scaricare gli script malevoli.

Di seguito vediamo la lista degli utenti Pastebin utilizzati ad agosto:

- halolu1
- alphabates3
- guccha
- passion1



Ransomware

Agosto 2020—ITALIA

Continuano gli attacchi ransomware utilizzando differenti vettori d'infezione.

Questo mese registriamo una diminuzione degli attacchi ransomware rispetto al mese scorso.

La nostra telemetria ha registrato gli attacchi dei seguenti ransomware:

- **Matrix**
- **LockBit**
- **Phobos**

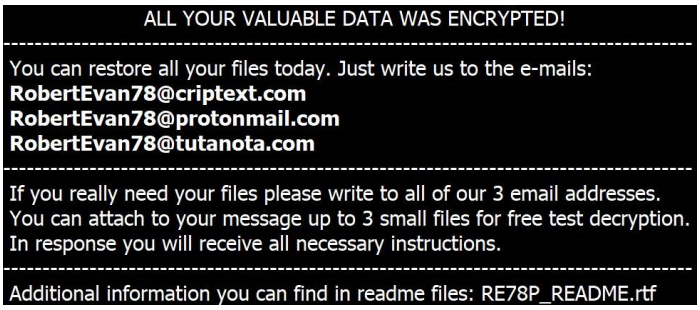
I ransomware identificati ad agosto derivano da attacchi attraverso il desktop remoto (RDP) mirati verso aziende italiane e navigazione su siti compromessi.

Gli attacchi via RDP mirati o "targettizzati" verso aziende italiane, permettono un accesso abusivo al sistema per eseguire direttamente il ransomware. In queste particolari situazioni il cybercriminale o attaccante cerca di disinstallare l'antivirus o di renderlo inoperativo, in modo che l'attacco ransomware abbia successo.

Matrix non è un ransomware nuovo, ne abbiamo già parlato nei mesi scorsi. L'attacco in questione è avvenuto via RDP tra la notte dell'uno e il due agosto, con la seguente cronologia di operazioni:

1. **2020-08-01 22:02:52** tentativo di disinstallazione dell'anti-virus;
2. **2020-08-02 02:54:50** tentativo di disattivazione della protezione anti-ransomware
3. **2020-08-02 02:56:00** esecuzione di GMER
4. **2020-08-02 03:08:00** primo tentativo di esecuzione del ransomware
5. **2020-08-02 03:35:00** secondo tentativo di esecuzione del ransomware
6. **2020-08-02 04:16:00** terzo tentativo di esecuzione del ransomware
7. **2020-08-02 04:38:00** quarto tentativo di esecuzione del ransomware

Nell'immagine sottostante possiamo vedere le istruzioni per la richiesta di riscatto dei file cifrati.



Il 19 agosto vi è stato un duplice attacco ransomware *LockBit-Phobos* mentre la vittima stava navigando molto probabilmente su siti compromessi. L'estensione dei file cifrati utilizzato dal ransomware Phobos durante l'attacco era **.ROGER.**

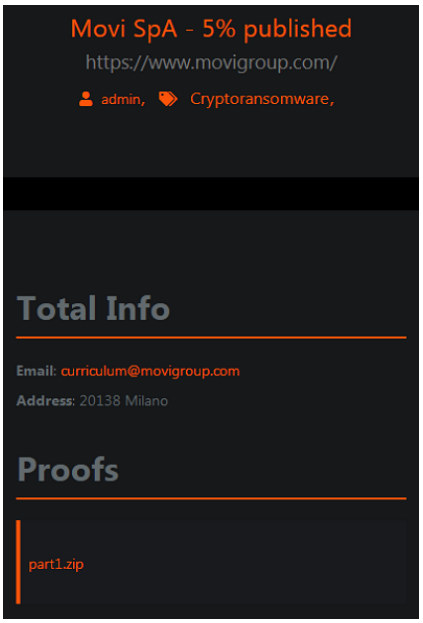
Il 30 agosto un altro attacco via RDP ha veicolato il ransomware **LockBit.** L'attacco ransomware veniva bloccato dalla protezione anti-ransomware andando ad inibire il processo di cifratura dei file.

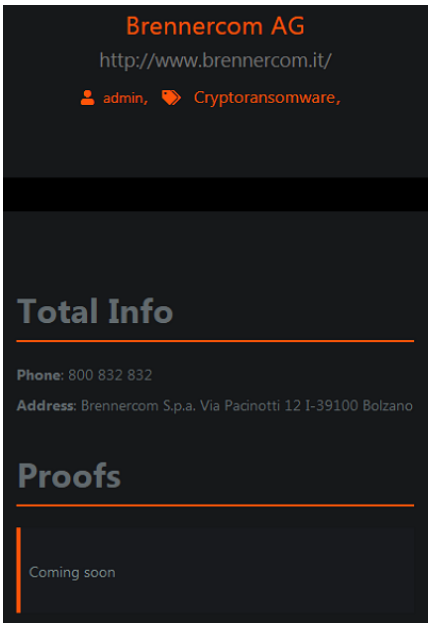
Probabilmente il cyber-criminale, collegato via RDP, si accorgeva che il suo attacco ransomware era fallito, ed indispettito provava a inibire l'accesso alla macchina con un blocco schermo con password, come in figura:

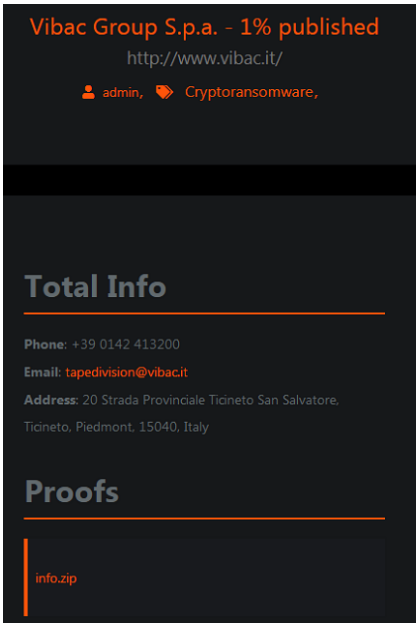
Ad agosto il gruppo cyber–criminale del **Maze** ha attaccato altre tre società italiane:

- Movi S.p.a. (Milano)
- Brennercom AG (Bolzano)
- Vibac Group S.p.a. (Ticineto – AL)

Sia per **Movi S.p.a.** (5%) sia per **Vibac Group S.p.a.** (1%) sono stati pubblicati una parte delle informazioni riservate esfiltrate durante l'attacco.



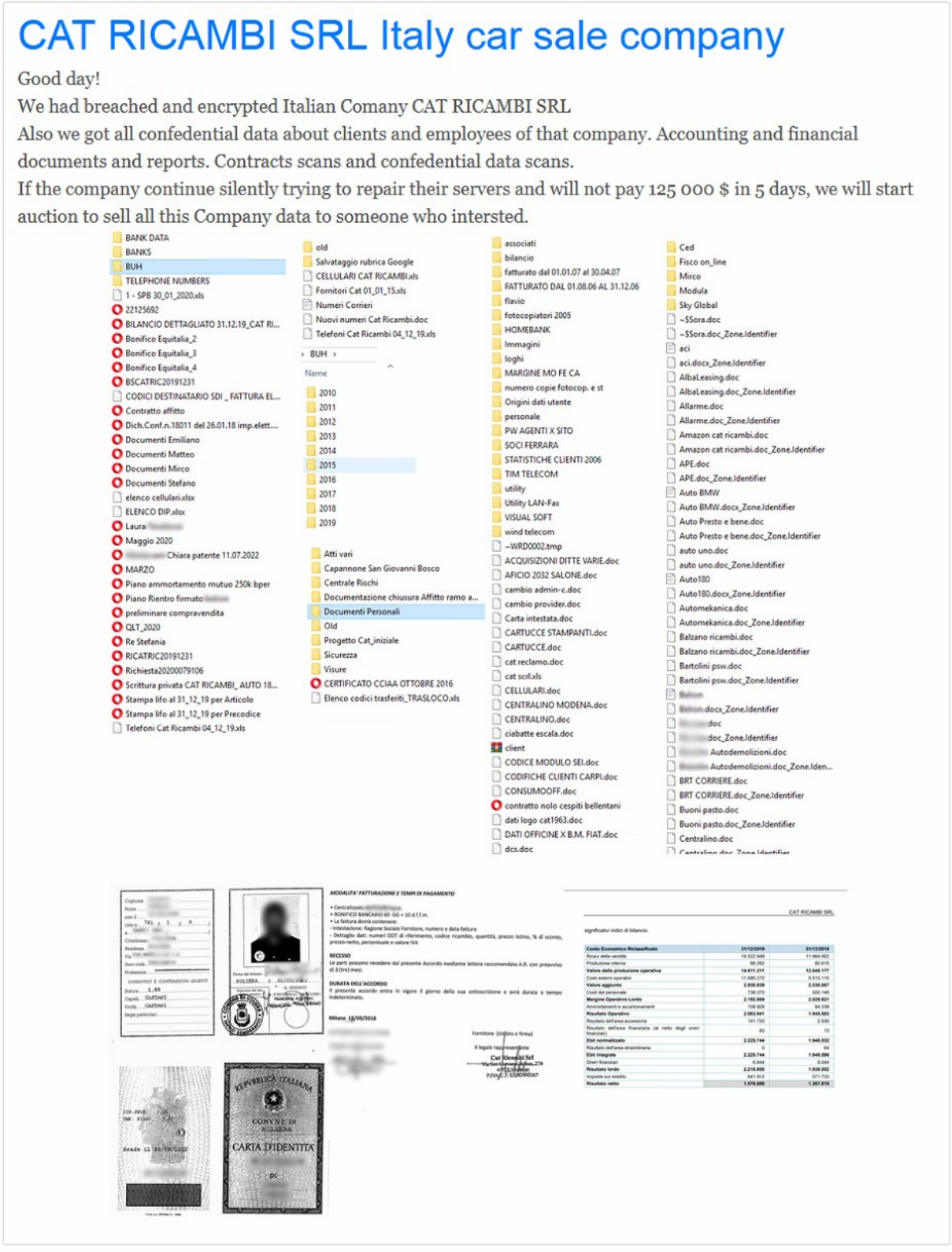




Per quanto riguarda il ransomware **Conti**, successore di **Ryuk**, i cyber-criminali affermano ad agosto di aver attaccato le società **Volkswagen** e **Peugeout Motorcycle** con esfiltrazione di documenti riservati, come mostrato nelle immagini sottostanti.

Ad agosto il gruppo cyber–criminale di **REvil** (aka **Sodinokibi**) ha colpito l'azienda italiana **CAT Ricambi S.r.l.** chiedendo un riscatto di **125.000 dollari** per non far partire l'asta dei dati esfiltrati.

REvil è salito alla ribalta per aver attaccato lo studio legale **Grubman Shire Meiselas & Sacks** delle star americane come **Jessica Simpson**, **Bruce Springsteen, Mariah Carey** e **Nicki Minaj**. Il pacchetto completo, che è attualmente all'asta, di 750 GB di dati esfiltrati, ha uno starting price di 21 milioni di dollari e un blitz price di 42 milioni.



Prevalenza

Agosto 2020—ITALIA

Quanto sono protetti i computer in Italia dagli attacchi informatici? Quanto è alto il rischio che un utente sia colpito da un ransomware ?

Per rispondere a queste domande dobbiamo parlare di "prevalenza" e "infection rate".

La prevalenza è un indice che ci permette di capire lo stato della Cyber-Security. Questo dato fornisce lo stato di "salute" dei computer, quantificando il numero di computer colpiti da malware.

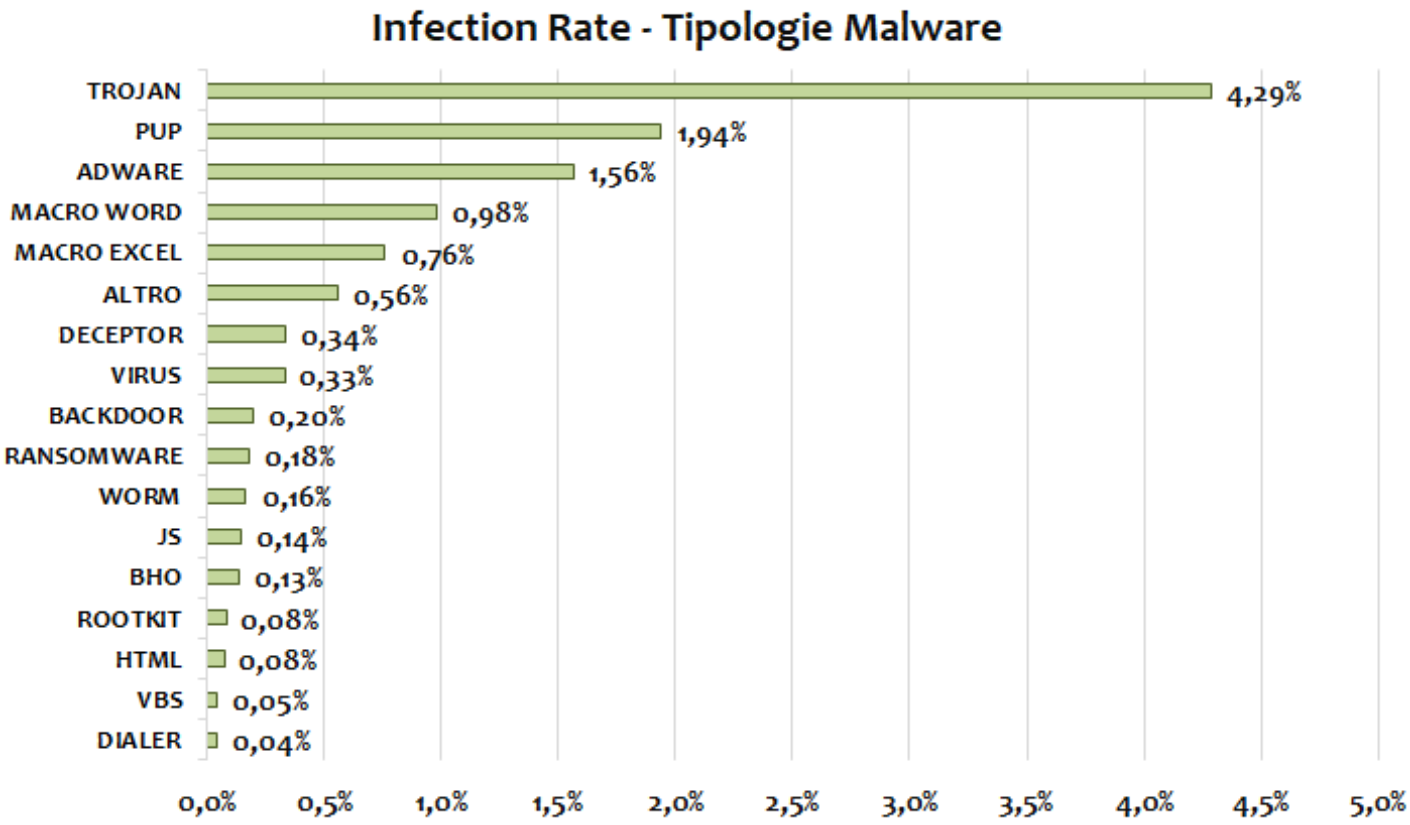
Vediamo ora i dati relativi alla prevalenza dei malware registrati dal C.R.A.M. di TG Soft nel mese di agosto 2020. Per prevalenza si intende l'incidenza che i malware hanno in un determinato periodo. Il valore calcolato si chiama "rate di infezione".

Il rate di infezione viene calcolato dividendo il numero di computer ove siano stati rilevati attacchi per il numero di computer dove è installato il software anti-virus Vir.IT eXplorer. Possiamo calcolare il rate di infezione per le seguenti categorie:

- Tipologia del malware
- Sistema operativo (client/server)

Al primo posto i **Trojan** con una percentuale del 4,29%. Secondo posto confermato per i **PUP** , con una percentuale dell'1,94%. Terzo gradino del podio per la categoria **Adware** con l'1,56%.

Dalla 4ª alla 6ª posizione troviamo i MacroVirus, con le macro di Excel e di Word, seguite dal gruppo generico denominato Altro (che include le macro di Office generiche). Si attestano in 10ª posizione i **Ransomware** con lo 0,18%. Sono considerati tra i malware più pericolosi se non addirittura i più incontrastabili qualora si fosse sprovvisti di tecnologie Anti-Ransomware. Ricordiamo che per Ransomware vengono considerati tutti i malware che chiedono un riscatto, come, ad esempio, i Crypto-malware (SodinoKibi, Phobos, LockBit etc.) e il vecchio e famoso FakeGDF (virus della polizia di stato, guardia di finanza etc.).

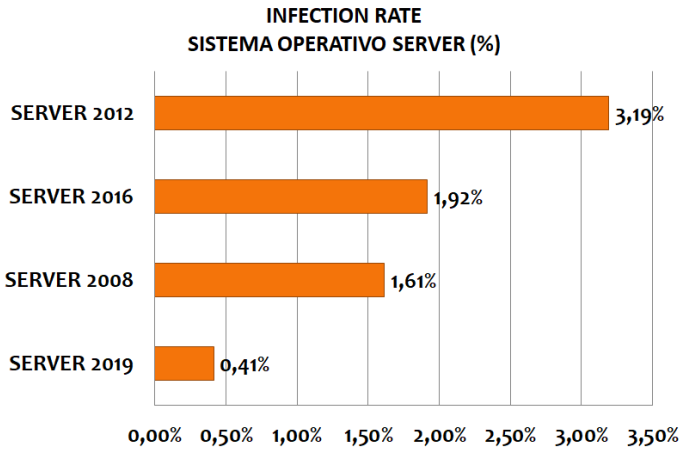


Andiamo ora ad analizzare la prevalenza delle infezioni del mese di agosto in base ai sistemi operativi suddivisi tra sistemi Server e Client.

Nelle immagini sottostanti i dati raccolti sono stati suddivisi secondo i sistemi operativi Windows Server e Client in macro categorie, senza dividere per tipo di architettura o per le varianti che la stessa versione può avere (es: Server 2008 R2, Server 2008 R2 Foundation, etc.), calcolati sulla totalità delle macchine rispettivamente server e client indicate.

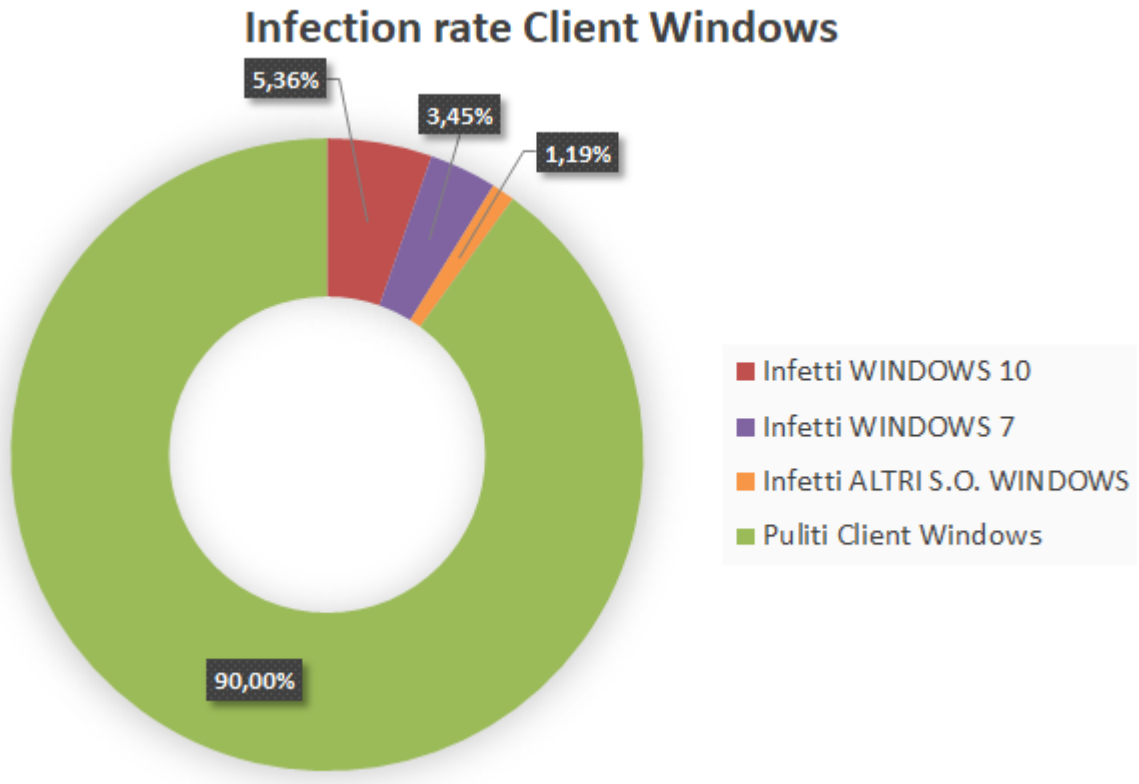
Dai dati relativi ai server, si potrebbe evincere che la probabilità dell'infezione/attacco di un Server 2019 rispetto ad un Server 2012 (più datato…) è di un ordine di grandezza inferiore 0,41% contro 3,19%.

Nelle statistiche relative alla prevalenza delle infezioni dei computer client nel mese di agosto abbiamo riscontrato che il **10%** dei terminali è stato infettato o ha subito un attacco. Questo dato indica che **1 computer su 10** è stato colpito da malware nel mese di agosto.



Nella figura sottostante possiamo vedere il grafico delle infezioni in base ai sistemi operativi dei Client, dove il campione analizzato è così composto:

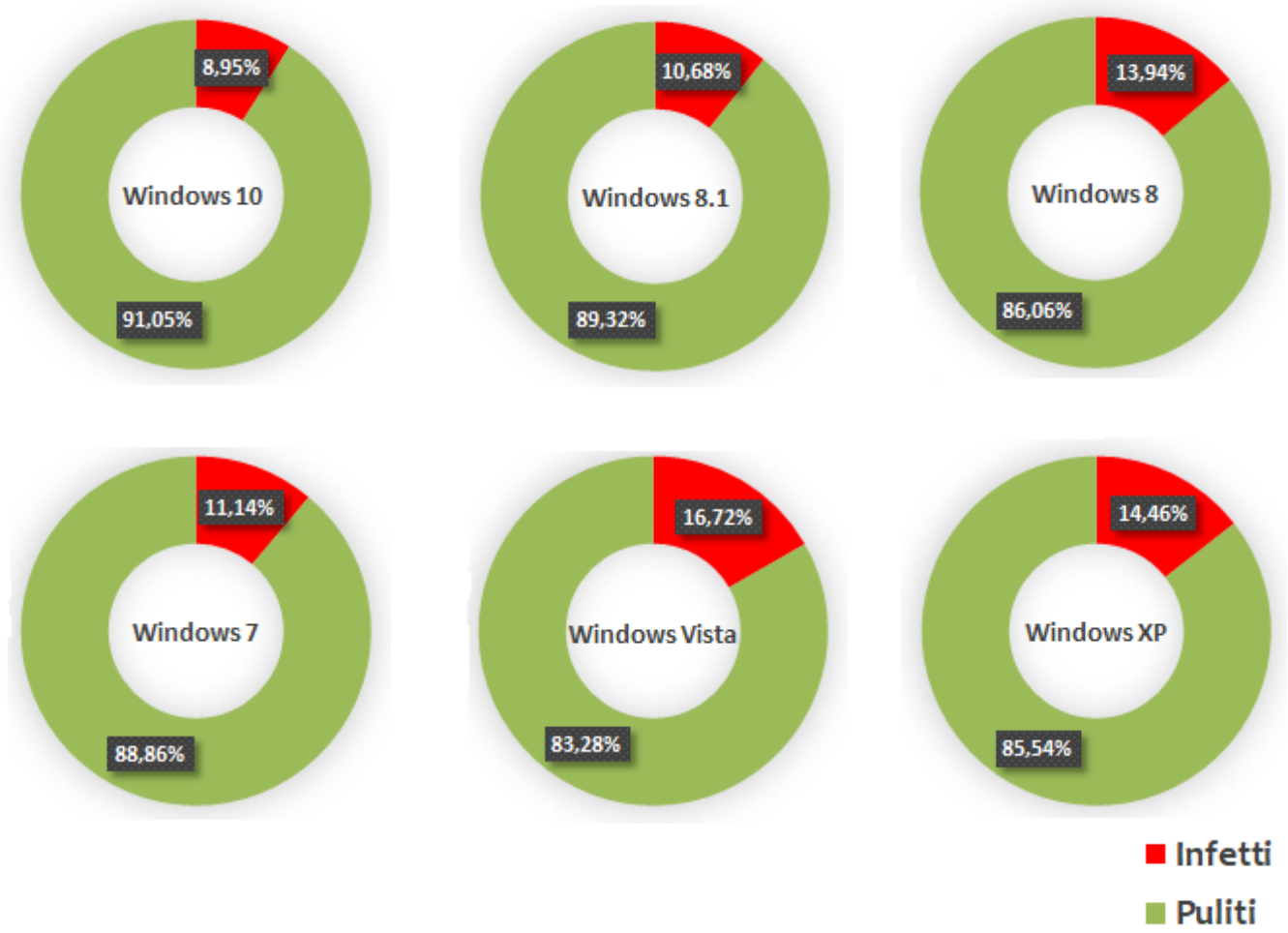
- 59,14% client con Windows 10
- 30,57% client con Windows 7
- 10,29% client con altri s.o. Windows



Windows 10 e **Windows 7** coprono quasi il 90% del parco macchine dei Client, pertanto gli altri sistemi operativi sono stati raccolti in un unico gruppo.

Ma quale sarà il sistema operativo più sicuro ?

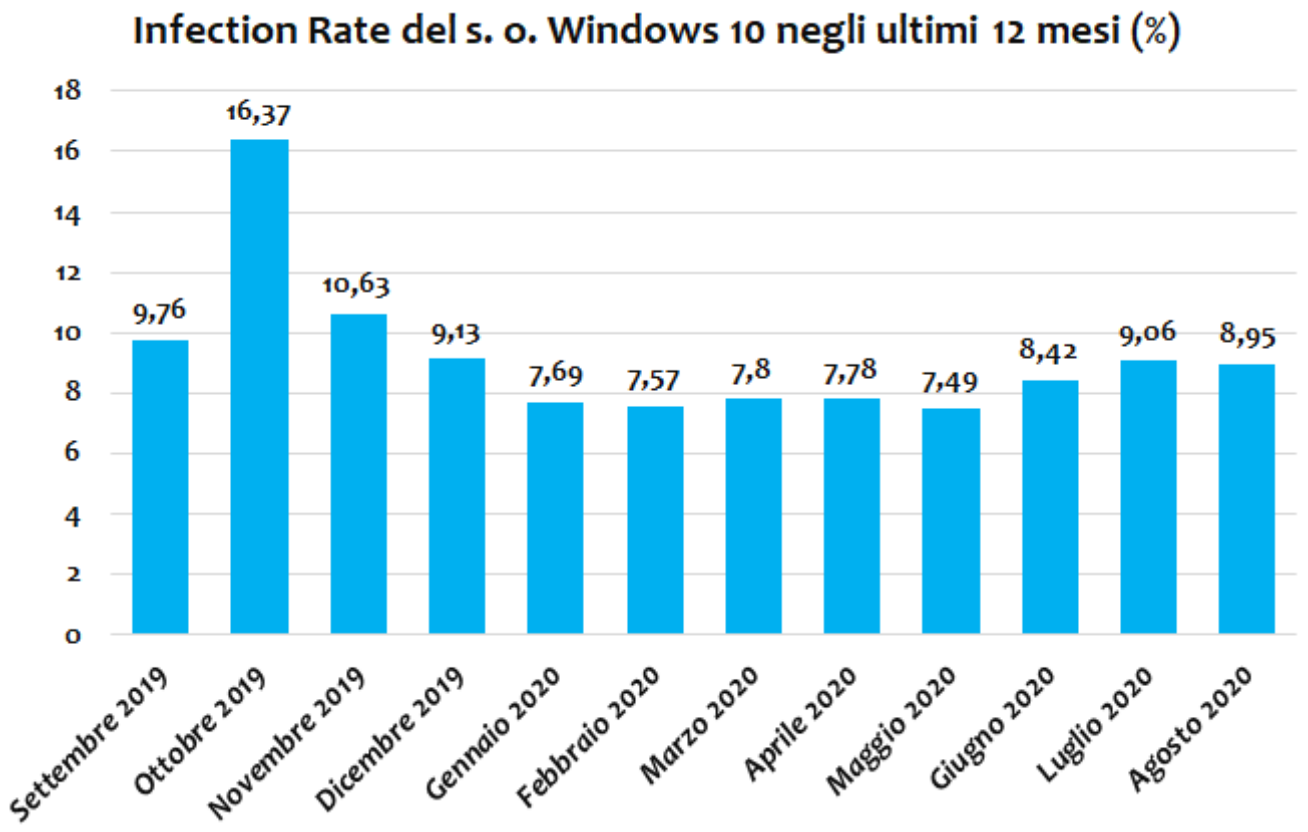
Per rispondere a questa domanda dobbiamo calcolare la prevalenza d'infezione sul medesimo sistema operativo. Prendendo ad esempio Windows 10, si può notare che il rate di infezione tra tutte le macchine ove è installato Windows 10 che ha subito un attacco informatico è dell'8,95% . Con questo calcolo possiamo capire quindi qual è il sistema operativo più sicuro.



Nei grafici a torta è stato calcolato l'Infection Rate (IR) relativo alla prevalenza sul medesimo sistema operativo client. Il sistema operativo che ha subito meno attacchi risulta essere Windows 10, questo dimostra che utilizzare sistemi operativi moderni e supportati riduce il rischio di infezione. I sistemi operativi non più supportati da Microsoft, come Windows XP e Vista, hanno di fatto il rate d'infezione molto più alto. Paragonando Windows Vista a Windows 10, si può notare infatti che l'IR è quasi il doppio.

Come ultimo grafico delle nostre statistiche, andiamo a vedere l'andamento dell'IR relativo al sistema operativo Windows 10 negli ultimi 12 mesi.

Il periodo di maggiore infezione è ottobre 2019. In quel periodo e anche nei mesi adiacenti erano massivamente diffuse campagne malware atte a distribuire i trojan Emotet e TrickBot. Da Gennaio 2020 la situazione a seguito della diminuzione delle campagne di Emotet/TrickBot sembrava essersi normalizzata. Nel mese di agosto registriamo un leggere calo delle infezioni rispetto al mese di luglio. Il mese di agosto 2020 è in linea con lo stesso mese dell'anno scorso, anche se abbiamo avuto un numero elevato di campagne di malspam, ma queste per ora non hanno così inciso su Windows 10, come era invece successo ad ottobre del 2019.



TG Soft
Cyber Security Specialist
www.tgsoft.it