Cyber-Threat Report

Ottobre 2020

TG Soft
Cyber Security Specialist
www.tgsoft.it

Ottobre 2020

TG Soft
Cyber-Threat Report

Notizie di rilievo:

QakBot

Panorama delle minacce in Italia a ottobre

Sommario:

Nel mese di ottobre si è riscontrato un incremento degli attacchi informatici ed una leggera crescita del numero dei cluster di malware rispetto al mese di settembre.
Emotet ha continuato le sue campagne di malspam verso l'utenza italiana ma con meno forza. Nonostante il calo del numero delle campagne, rimane uno dei malware più diffusi e pericolosi in Italia.

Nelle prime due settimane abbiamo una diversificazione degli attacchi malware, grazie alla pausa di Emotet. Nelle settimane successiva Emotet ha ripreso, ma molto lentamente e ha veicolato **QakBot**.
Ursnif è stato molto attivo con diverse campagne per tutto ottobre. Tra i password stealer sugli scudi: **AgentTesla; FormBook** e **Remcos**.
Anche il cyber-attore **Hagga** non ci ha fatto mancare la sua presenza, anche in Italia.
Sono continuati gli attacchi RDP che hanno veicolato i ransomware **Dharma, Phobos** e **ShivaGood**.

CRAM
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

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.

Proteggiamo il tuo business dai cyber-criminali

[www.tgsoft.it]

Seguici sui 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.

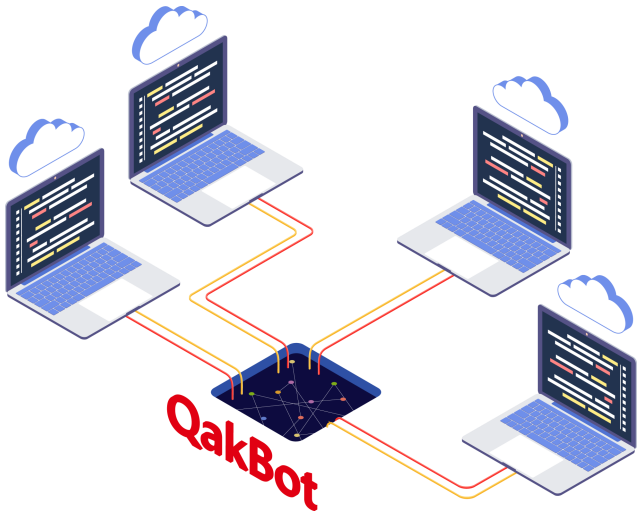
L'indice che misura lo stato della Cyber-Security è l'Infection Rate (IR), che è la percentuale degli utenti dell'anti-virus Vir.IT eXplorer che hanno incontrato una minaccia che sia stata segnalata al C.R.A.M. di TG Soft.

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

QakBot



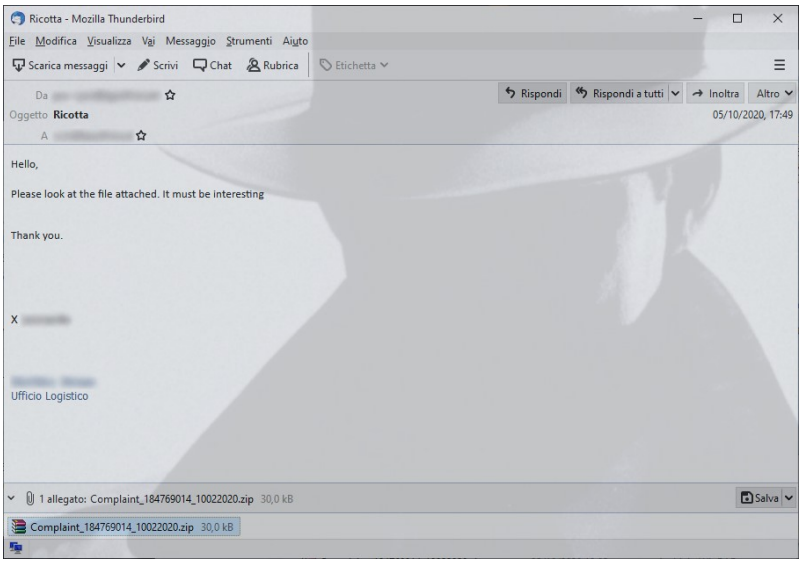
QakBot non è un malware nuovo ed è stato scoperto più di 10 anni fa, ma è tornato in auge quando a luglio Emotet è risorto. A partire da metà luglio Emotet ha iniziato a diffondere attraverso il sistema MasS (Malware-as-a-Service) il malware QakBot, nei mesi precedenti veniva diffuso attraverso la propria botnet principalmente il malware TrickBot. Nell'ultimo periodo però questa tendenza è cambiata, ed Emotet ha iniziato a diffondere la triade QakBot, TrickBot e ZLoader in base alle particolari aree geografiche.

QakBot è considerato un trojan banker, che è in grado di rubare credenziali di accesso, password ed esfiltrare dati, con capacità di worm per diffondersi da un computer all'altro nella stessa rete (spostamento laterale).

Negli ultimi mesi QakBot si è diffuso in Italia attraverso:

- Botnet di Emotet;
- Campagne di malspam dirette.

Nella figura a lato possiamo vedere un esempio di campagna malspam del 5 ottobre 2020 che ha veicolato QakBot.

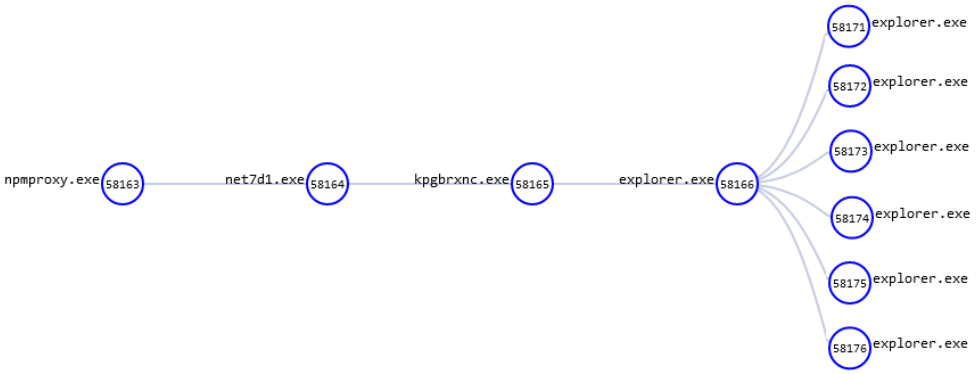


Ma la maggiore diffusione di QakBot in Italia è avvenuta attraverso la botnet di Emotet, poche sono state le campagne monitorate in Italia rispetto ai sample diffusi attraverso Emotet.

QakBot è un malware complesso, che oltre all'esfiltrazione dati può scaricare anch'esso altri malware.

L'esempio analizzato è stato scaricato sul computer della vittima attraverso il malware Emotet.

In figura possiamo vedere lo schema d'infezione.



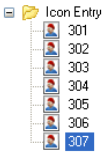
La catena d'infezione inizia quando Emotet (npmproxy.exe) riceve il comando dal server C&C per scaricare il malware QakBot (net7d1.exe). Il file del malware viene salvato da Emotet nella stessa cartella e poi eseguito. QakBot si copia all'interno di una cartella con nome casuale (kpgbrxnc.exe):

C:\%username%\AppData\Roaming\Microsoft\<cartella casuale>\<nome casuale>.exe

Il file di partenza di QakBot all'interno della cartella di Emotet, viene sovrascritto con il file CALC.EXE, attraverso il seguente comando:

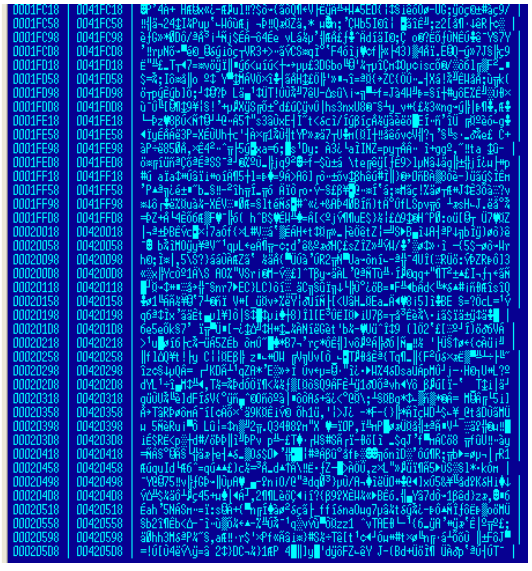
```
"C:\Windows\System32\cmd.exe"  /c ping.exe -n 6 127.0.0.1 &  type
"C:\WINDOWS\System32\calc.exe" > "C:\%username%\APPDATA\Local\<Folder
di Emotet>\<nome del file qakbot>.exe"
```

Il comando non fa altro che eseguire 6 volte il ping e dopo sovrascrive il file di partenza del qakbot.

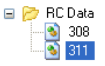


A questo punto QakBot esegue Explorer.exe per iniettarsi all'interno, da dove poi contatterà i propri server C2 per scaricare nuove versioni e/o inviare i dati esfiltrati dal computer della vittima.

Il file eseguibile contiene diverse risorse cifrate numerate dal 301 al 307. La risorsa 307 contiene il payload da iniettare nel processo Explorer.exe.



A sua volta, il payload iniettato contiene altre due risorse cifrate con RC4, come possiamo vedere nella figura a lato. La risorsa 308 contiene la configurazione iniziale di QakBot, invece la risorsa 311 contiene la lista dei server di comando e controllo (150 indirizzi ip).



In figura a lato, possiamo vedere la configurazione di QakBot, che contiene due parametri (10 e 3). Il parametro 10 indica l'ID della campagna, in questo caso il suo valore è *partner01* che è associato a Emotet, il secondo parametro 3 indica un timestamp (2020-07-29 14:25:25).

```
00: 6A 46 F1 D0  A8 34 9E 52  58 3F 36 40  DC A5 32 C7 jF...4.RX?6@..2.
10: 7C 02 97 17  31 30 3D 70  61 72 74 6E  65 72 30 31 |...10=partner01
20: 0D 0A 33 3D  31 35 39 36  30 33 32 37  32 35 0D 0A ..3=1596032725..
```

La persistenza di QakBot viene ottenuta attraverso l'esecuzione di task e l'aggiunta di chiavi di registro:

- "C:\WINDOWS\system32\schtasks.exe" /create /tn {1AD734C2-0803-4F04-94C8-7CBCC6628FFA} /tr "\"C:*%username%*\AppData\Roaming\Microsoft\<random folder>\<random name>.exe\"" /sc HOURLY /mo 5 /F
- "C:\WINDOWS\system32\schtasks.exe" /create /tn {7F7ABA39-470D-4E0C-9A90-D911E8D9BFFA} /tr "cmd.exe /C \"start /MIN C:\WINDOWS\system32\cscript.exe //E:javascript \"C:*%username%*\<random name>.npl\"\" sudhfdus" /sc WEEKLY /D TUE,WED,THU /ST 12:00:00 /F
- HKCU\Software\Microsoft\Windows\CurrentVersion\Run\<random> -> c:\%username%\AppData\Roaming\Microsoft\<cartella casuale>\<nome casuale>.exe

Il file .npl è uno script che andrà ad eseguire il file del QakBot.

Nella cartella di QakBot possiamo trovare diversi file:

- .dat -> contiene la configurazione della rete della vittima
- .dll -> contengono le informazioni esfiltrate alla vittima

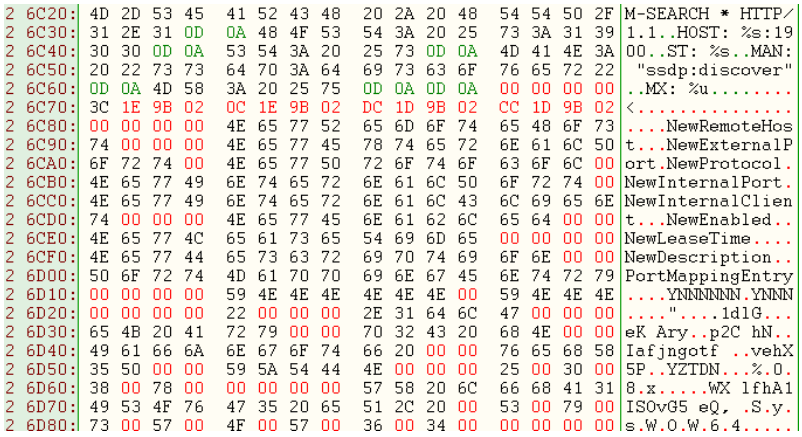
Nella figura sotto possiamo vedere un file .dat di configurazione della rete di una vittima. Anche in questo caso vi sono diversi parametri: 10, 11, 1, 2, 50, 14, 49, 45, 46, 39, 6 e 38.

```
    00 01 02 03  04 05 06 07  08 09 0A 0B  0C 0D 0E 0F  0123456789ABCDEF
000: 5A 12 43 6E  48 7E 9C F5  E9 B3 0C 4B  CF 91 84 C0 Z.CnH~.....K....
010: 08 BE 8C 02  31 30 3D 70  61 72 74 6E  65 72 30 31 ....10=partner01
020: 0D 0A 31 31  3D 32 0D 0A  31 3D 31 37  2E 34 35 2E ..11=2..1=17.45.
030: 31 34 2D 30  34 2F 30 39  2F 32 30 32  30 0D 0A 32 14-04/09/2020..2
040: 3D 31 35 39  39 32 33 34  33 31 34 0D  0A 35 30 3D =1599234314..50=
050: 31 0D 0A 31  34 3D 31 30  3B 38 3B 31  35 39 39 35 1..14=10;8;15995
060: 38 35 35 37  31 7C 35 3B  31 3B 31 35  39 39 35 38 85571|5;1;159958
070: 35 38 32 32  7C 34 32 39  34 39 36 37  32 39 35 3B 5822|4294967295;
080: 32 33 3B 31  35 39 39 32  33 34 33 34  39 7C 33 30 23;1599234349|30
090: 30 3B 31 33  3B 31 35 39  39 35 37 37  38 32 34 7C 0;13;1599577824|
0A0: 32 37 33 36  3B 33 3B 31  35 39 39 35  36 36 36 34 2736;3;159956664
0B0: 36 7C 33 3B  32 31 3B 31  35 39 39 35  38 35 38 32 6|3;21;159958582
0C0: 32 7C 34 32  39 34 39 36  37 32 39 35  3B 31 32 3B 2|4294967295;12;
0D0: 31 35 39 39  32 33 35 32  38 36 0D 0A  34 39 3D 31 1599235286..49=1
0E0:                                                    ..45=172.
0F0:                                                    ..46=443..39=5
100:                                                    .       ..6=5
110:                                                    4.      :654
120: 30 30 0D 0A  33 38 3D 31  35 39 39 32  33 35 33 32 00..38=159923532
130: 32 0D 0A 35  3D 54 41 42  42 41 46 41  41 56 41 42 2..5=TABBAFAAVAB
140: 50 41 46 41  41 4C 51 41  33 41 44 59  41 4E 41 41 PAFAALQA3ADYANAA
150: 7A 41 46 55  41 55 77 42  4E 41 46 55  41 4F 77 41 zAFUAUwBNAFUAOwA
160: 79 41 48 77  41 54 41 42  42 41 46 41  41 56 41 42 yAHwATABBAFAAVAB
170: 50 41 46 41  41 4C 51 42  47 41 45 55  41 4F 41 42 PAFAALQBGAEUAOAB
180: 55 41 46 4D  41 4E 67 41  35 41 44 41  41 4F 77 41 UAFMANgA5ADAAOwA
190: 78 41 48 77  41 55 77 42  46 41 46 49  41 56 67 42 xAHwAUwBFAFIAVgB
1A0: 46 41 46 49  41 4F 77 41  31 41 41 3D  3D 0D 0A    FAFIAOwA1AA==..
```

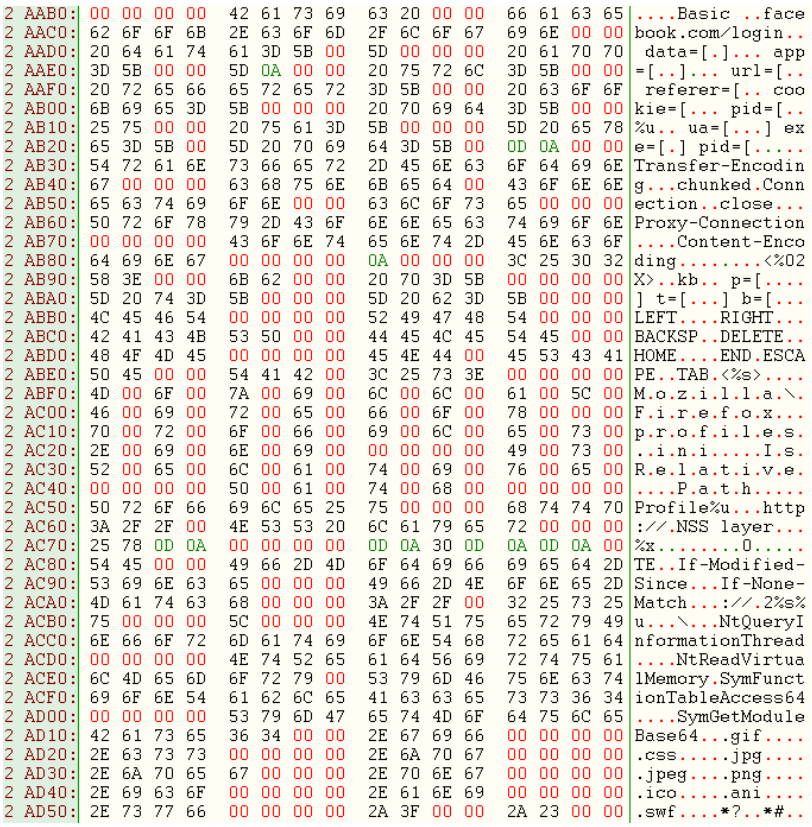
All'interno del processo di Explorer.exe possiamo trovare vari moduli di QakBot, che includono le principali funzioni:

- Esfiltrazione dati;
- Modulo worm.

Nella figura a destra, possiamo vedere i comandi SOAP per la richiesta al firewall di aprire una specifica porta ed inoltrarla ad esso e la stringa SSDP (Simple Service Discovery Protocol) per individuare dispositivi Plug & Play.



Invece nella figura sottostante possiamo vedere il dump del modulo di esfiltrazione dati di QakBot. Le informazioni esfiltrate saranno memorizzate in file cifrati con estensione .dll all'interno della cartella di QakBot ed inviati al server di comando e controllo.



Le comunicazioni con i server di comando e controllo avvengono in forma cifrata BASE64 + RC4, possiamo vedere un esempio decifrato di invio (a sinistra) e di risposta (a destra):


```
{    "8":1,
     "5":7,
     "1":17,
     "59":0,
     "3":"partner01",
     "4":805,
     "10":"1596032725",
     "2":"<omissis>",
     "6":40767,
     "14":"O6etCihSbMLi3WDjfoQ0ADyD244F6x5IMMjWE",
     "7":46062
}
```

```
{    "8":5,
     "16":1354157717,
     "39":"UdOVPwI6PrbqBy0pi0n6mKFtHbgAtw",
     "38":1
}
```


QakBot è un malware complesso, che oltre ad esfiltrare dati della vittima, potrebbe essere usato anche come punto di ingresso da altri cyber-criminali per sferrare attacchi all'intera rete aziendale. Questa ipotesi non è da escludere visti gli ultimi attacchi ransomware subiti da importanti società a livello mondiale. Lo "sharing" di informazioni ahimè non avviene solamente tra ricercatori anti-malware, ma anche tra attori cyber-criminali che possono "scambiarsi" informazioni sulla rete infettata, specialmente nel caso che la rete colpita sia di una certa importanza. QakBot è stato collegato al ransomware **ProLock**, ma non si esclude una possibile connessione con altri attori di ransomware.

Statistiche Malware

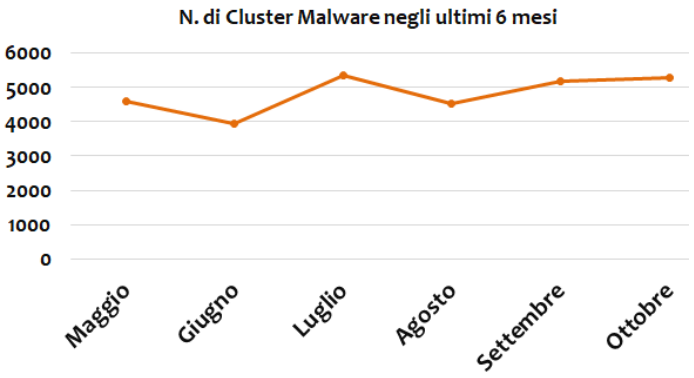
Ottobre 2020—ITALIA

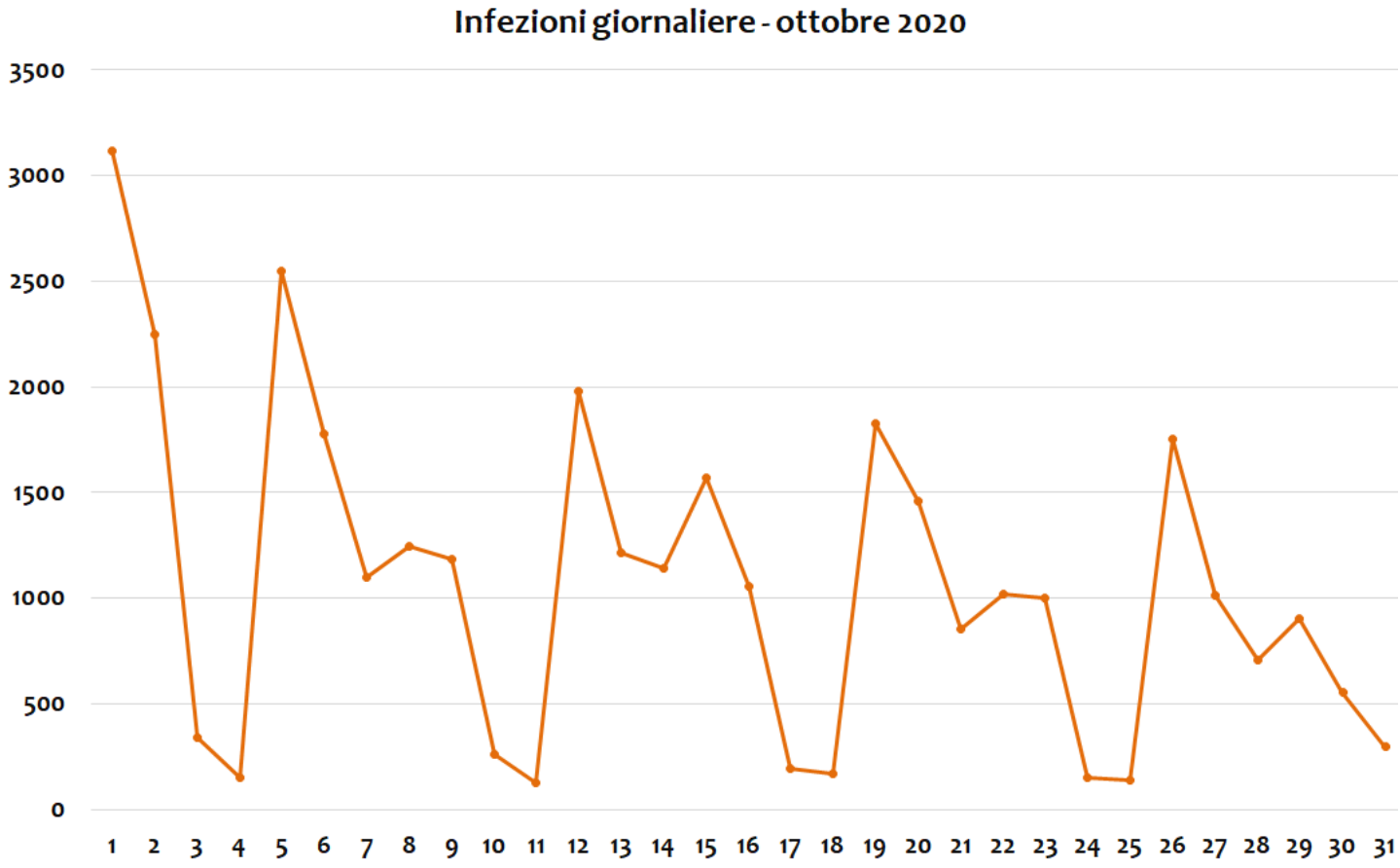
I dati della telemetria del C.R.A.M. di TG Soft sono raccolti dagli utenti che utilizzano il software anti-virus Vir.IT eXplorer. Le segnalazioni derivano da attacchi bloccati oppure malware riscontrati all'interno del parco macchine monitorato. Ogni minaccia identificata da Vir.IT viene classificata 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 ottobre abbiamo avuto un leggero incremento del numero di malware rispetto al precedente mese di settembre, dove erano stati riscontrati 5195 cluster di malware contro i 5280 del mese di ottobre (+1,6%).

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

All'inizio del mese abbiamo avuto un picco di segnalazioni d'infezione, dovute alle scansioni automatiche mensili del motore anti-virus Vir.IT eXplorer. Nelle settimane successive, abbiamo un incremento delle segnalazioni ogni lunedì e giovedì, per poi calare in modo progressivo nei giorni successivi. L'andamento delle infezioni a ottobre è stato abbastanza uniforme, non vi sono stati attacchi massivi come era successo a settembre, poiché Emotet ha deciso di non colpire pesantemente l'Italia, ma invece di interessarsi ad altri stati come la Romania e la Grecia.





Nel grafico sottostante vediamo le statistiche relative al mese di ottobre 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.

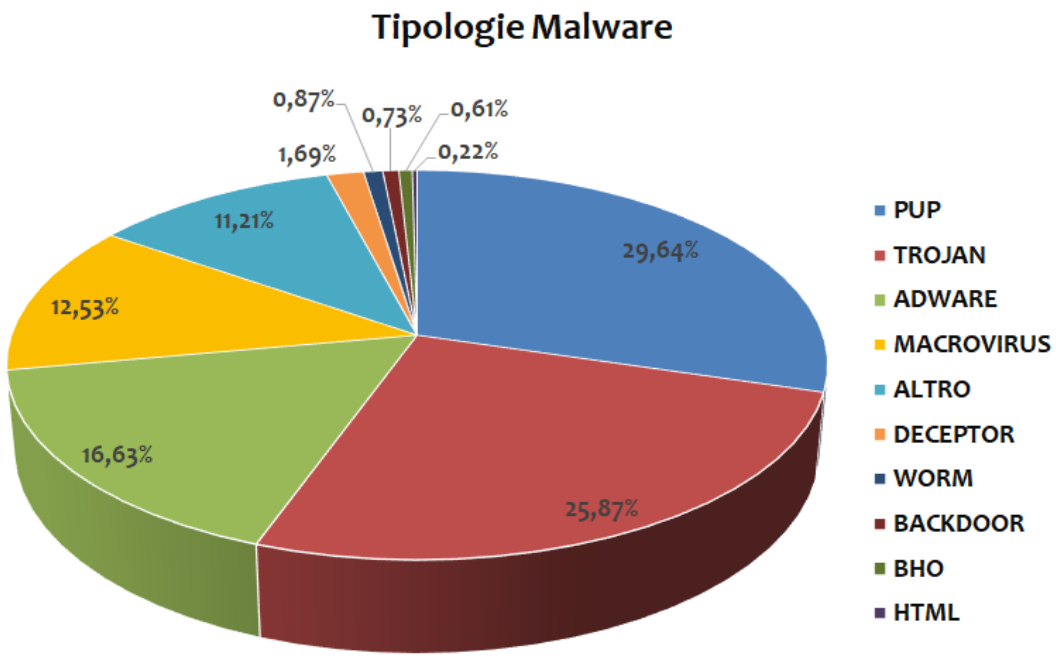
I malware si suddividono in diverse tipologie: Adware, Backdoor, Trojan, Worm, Virus, PUA/PUP, Deceptor, etc.

Nel mese di ottobre la tipologia dei **PUP** ritorna in prima posizione con il 29,64% delle infezioni, relegando la famiglia dei **TROJAN** al secondo posto con il 25,87%. Al terzo posto troviamo gli **ADWARE** con il 16,63% in crescita rispetto a settembre. I **MACROVIRUS** scendono dalla prima posizione di settembre alla quarta. Questo calo dei MACROVIRUS dipende dallo scarso volume di malspam generato da Emotet in Italia, che ha portato ad un drastico calo d'infezioni.

E' interessante notare che le prime 4 tipologie di malware rappresentano quasi l'85% delle infezioni monitorate.

Al quinto posto troviamo il gruppo denominato **ALTRO**, che include i virus, con l'11,21% delle infezioni in leggera crescita rispetto al mese scorso. In sesta posizione troviamo anche questo mese i **DECEPTOR** con l'1,69%, seguono **WORM** con lo 0,87% e chiudono la classifica: **BACKDOOR; BHO** e **HTML.**

I PUP riconquistano la prima posizione, brusco calo della famiglia dei MACROVIRUS, dovuto alla diminuzione del volume di malspam in Italia di Emotet.



Analizziamo le statistiche di ottobre dei singoli Malware. Questo mese ritorna al primo posto il **PUP.Win32.MindSpark.F** con il 6,01% delle infezioni, che può compromettere il tuo browser, modificando l'home page e il motore di ricerca.

Al secondo posto troviamo il de-troneggiato **Office.VBA_Macro_Heur** (tipologia MACRO VIRUS) con il 4,35% delle infezioni, in forte decremento di quasi 12 punti percentuali rispetto al mese scorso.

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**.

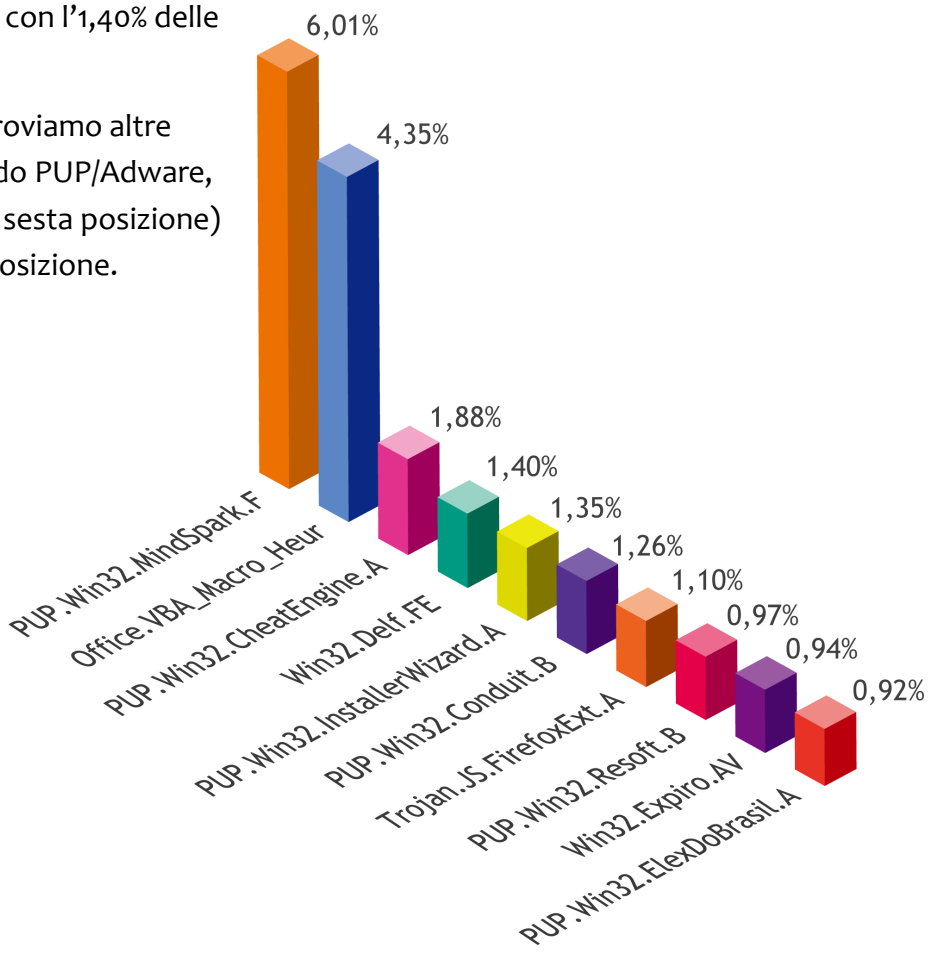
Al terzo posto troviamo il **PUP.Win32.CheatEngine** con l'1,88% delle infezioni rilevate. In quarta posizione troviamo una vecchia conoscenza il virus **Win32.Delf.FE** con l'1,40% delle infezioni.

Anche questo mese nella Top10 troviamo altre due vecchie conoscenze del mondo PUP/Adware, sono il **PUP.Win32.Counduit.B** (in sesta posizione) e il **PUP.Win32.Resoft** in ottava posizione.

I malware della Top10 rappresentano il 20,18% delle infezioni di ottobre, il rimanente 79,82% è dato da altri 5270 cluster di malware.

Nella Top10 troviamo ben 6 tipologie differenti di PUP, 2 tipologie virus , la tipologia dei macrovirus generici e un'estensione di Firefox generica.

I malware della Top10 rappresentano il 20,18% delle infezioni del mese di ottobre, il rimanente **79,82%** è dato da altri 5270 cluster di malware.

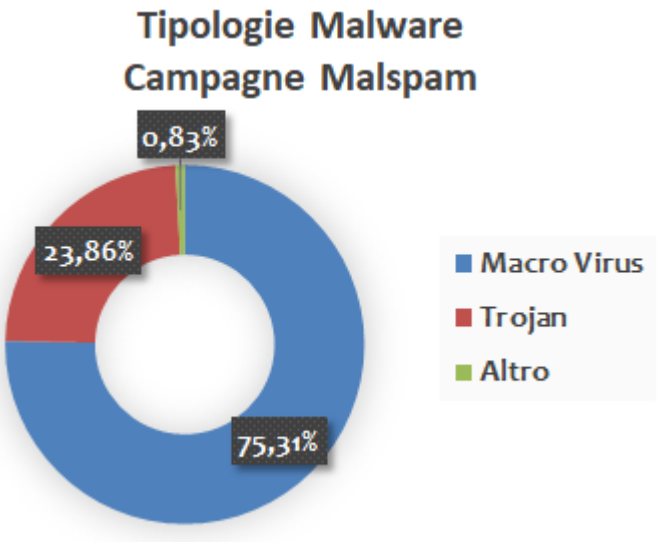


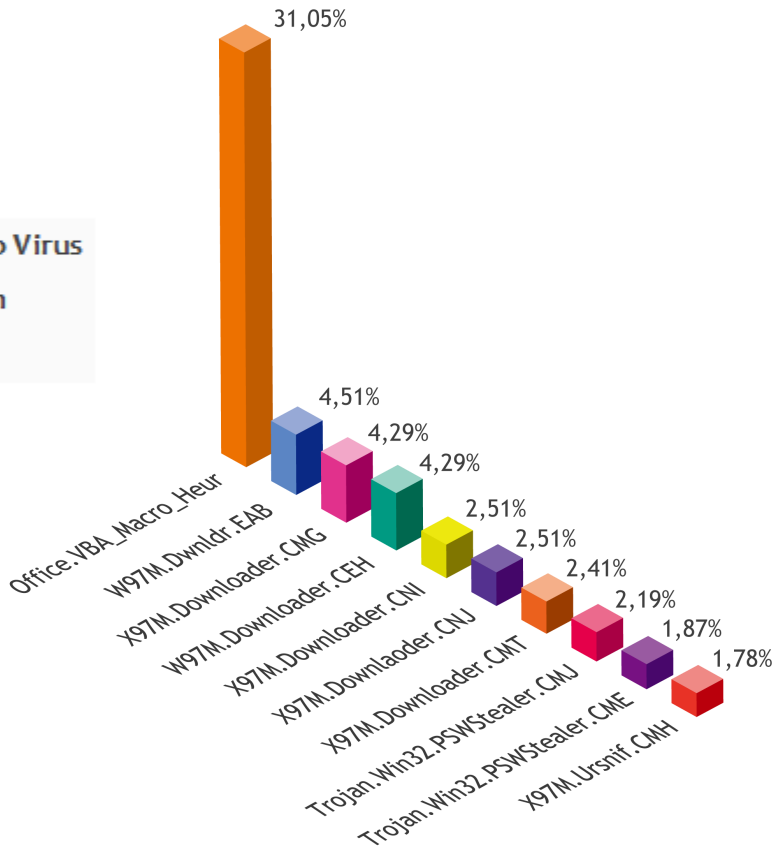
Statistiche Malware via email

Ottobre 2020—ITALIA

Analizziamo ora le campagne di malware veicolate via email nel mese di ottobre. 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 75,31% (-14,29%). Il dato ottenuto, segna un calo rispetto al mese scorso, grazie alla forte riduzione delle massive campagne di malspam di Emotet. Seguono la tipologia dei **TROJAN** che con il 23,86% (+13,5%) si confermano al secondo posto. Al terzo posto troviamo la tipologia **ALTRO** con lo 0,83% 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 l'intercettazione generica del malware **Emotet** con il 31,05%, in calo di quasi 30 punti. Al secondo posto troviamo **W97M.Dwnldr.EAB** con il 4.51% delle infezioni. Al terzo posto a pari merito troviamo **X97M.Downloader.CMG** e **W97M.Downloader.CEH** con il 4,29%. Dalla 5ª alla 7ª seguono 3 varianti di **X97M.Downloader**.

In 8ª e 9ª posizione troviamo due password stealer. Chiude in decima posizione il trojan bancario chiamato **Ursnif** con la varianti **.CMH**.

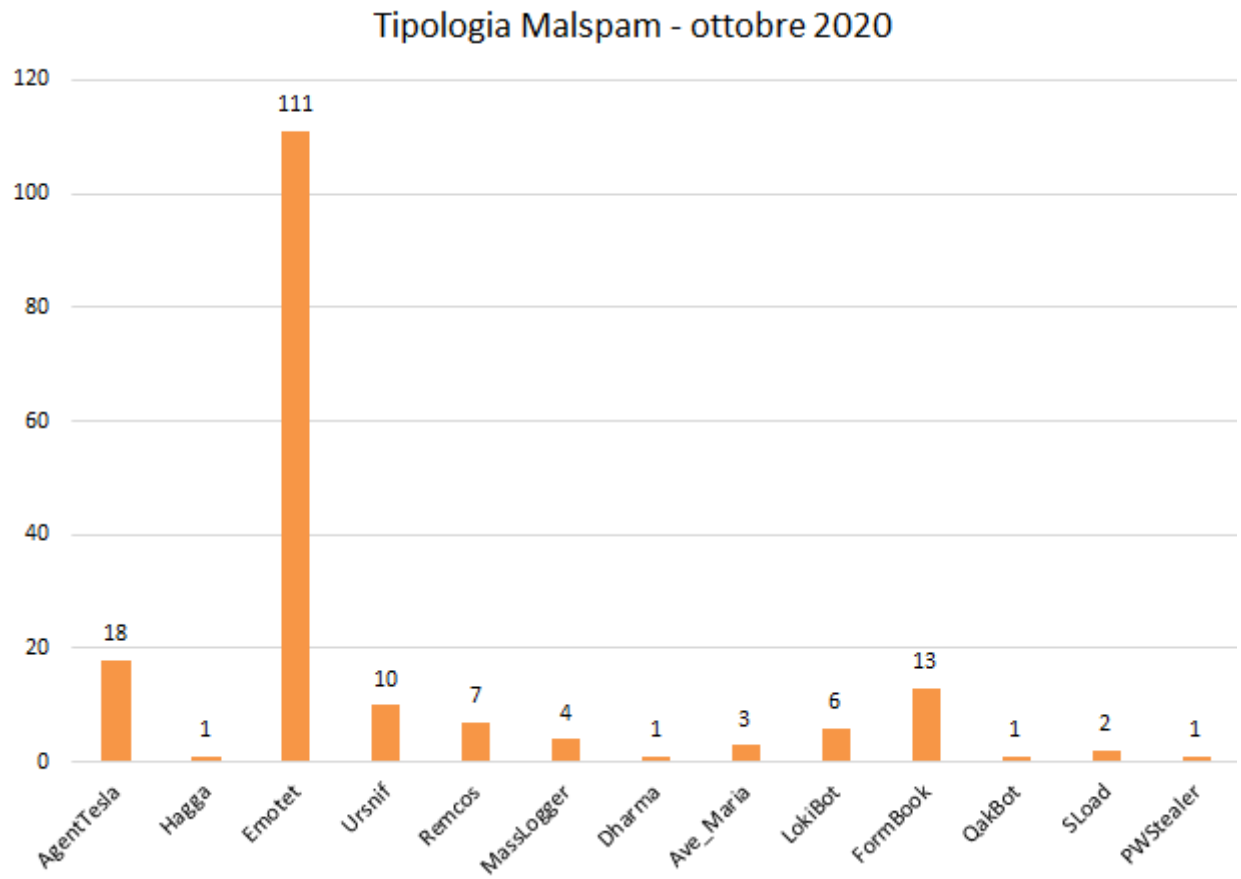
Nella Top10 delle mail, troviamo quasi esclusivamente MACRO VIRUS, che rappresentano il 53,35% delle infezioni di ottobre, il rimanente 46,65% è dato da altri 264 malware.

A ottobre il forte calo di Emotet in Italia ha portato ad una diminuzione delle infezioni da macro virus rispetto al mese di settembre.

Analisi dei malware di ottobre

Nel mese di ottobre in Italia, attraverso le campagne di malspam che hanno "targettizzato" l'utenza italiana (email scritte in lingua italiana), sono stati veicolati 13 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 ottobre.



A ottobre **Emotet** regna incontrastato con 111 campagne di malspam contro l'utenza italiana e si aggiudica la prima posizione. Emotet è un trojan downloader che può scaricare altri malware nel computer della vittima, come ad esempio QakBot, TrickBot e ZLoader.

Si riconferma in seconda posizione **AgentTesla,** un password stealer che ruba le credenziali di accesso, risulta essere molto utilizzato da diversi attori cyber-criminali nel mese di ottobre.

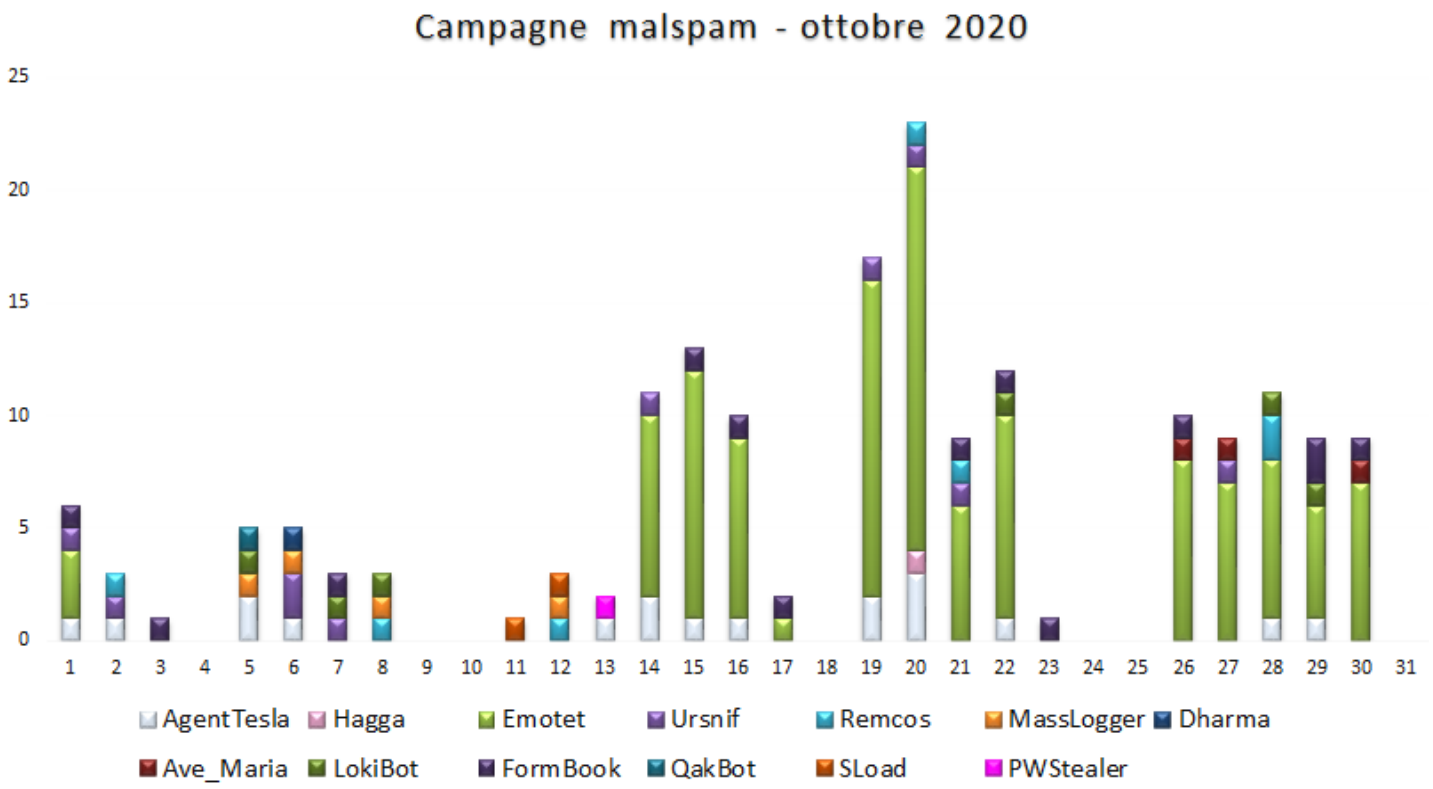
FormBook continua ad essere molto utilizzato e lo troviamo con ben 13 campagne. Invece il trojan banker **Ursnif** è risultato molto attivo rispetto a settembre, con 10 campagne. Lo scopo di questo malware è di rubare le credenziali di accesso all'home banking per svuotare il conto corrente.

A ottobre abbiamo registrato una campagna del ransomware Dharma, che di solito viene utilizzato negli attacchi via RDP.

Sono continuate le campagne di **QakBot, SLoad, Ave_Maria** e **LokiBot**. Ad ottobre è stata monitorata una campagna del cyber-attore **Hagga** che, assente a settembre, è tornato a colpire con le medesime tecniche viste nei mesi precedenti con allegato un documento infetto di PowerPoint che, questa volta, ha scaricato **AgentTesla**.

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

Nel mese di ottobre Emotet ha "spammato" solamente nella seconda metà del mese con un volume tendente al basso in Italia. Ogni settimana di ottobre sono state monitorate campagne di AgentTesla, FormBook e Ursnif in modo uniforme. Il picco delle campagne nel mese è avvenuto martedì 20 ottobre , dove sono state diffuse 23 campagne di malspam, che hanno veicolato 5 differenti famiglie di malware.



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

Week 39 ==> dal 26 settembre al 2 ottobre

Week 40 ==> dal 3 al 9 ottobre

Week 41 ==> dal 10 al 16 ottobre

Week 42 ==> dal 17 al 23 ottobre

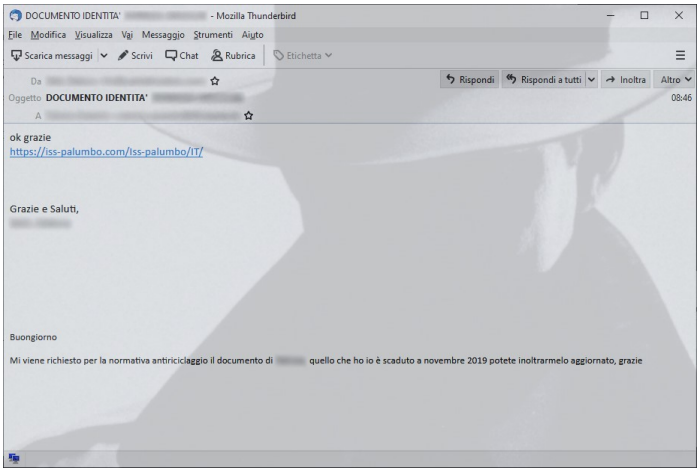
Week 43 ==> dal 24 al 30 ottobre

Emotet

Analisi delle campagne di ottobre

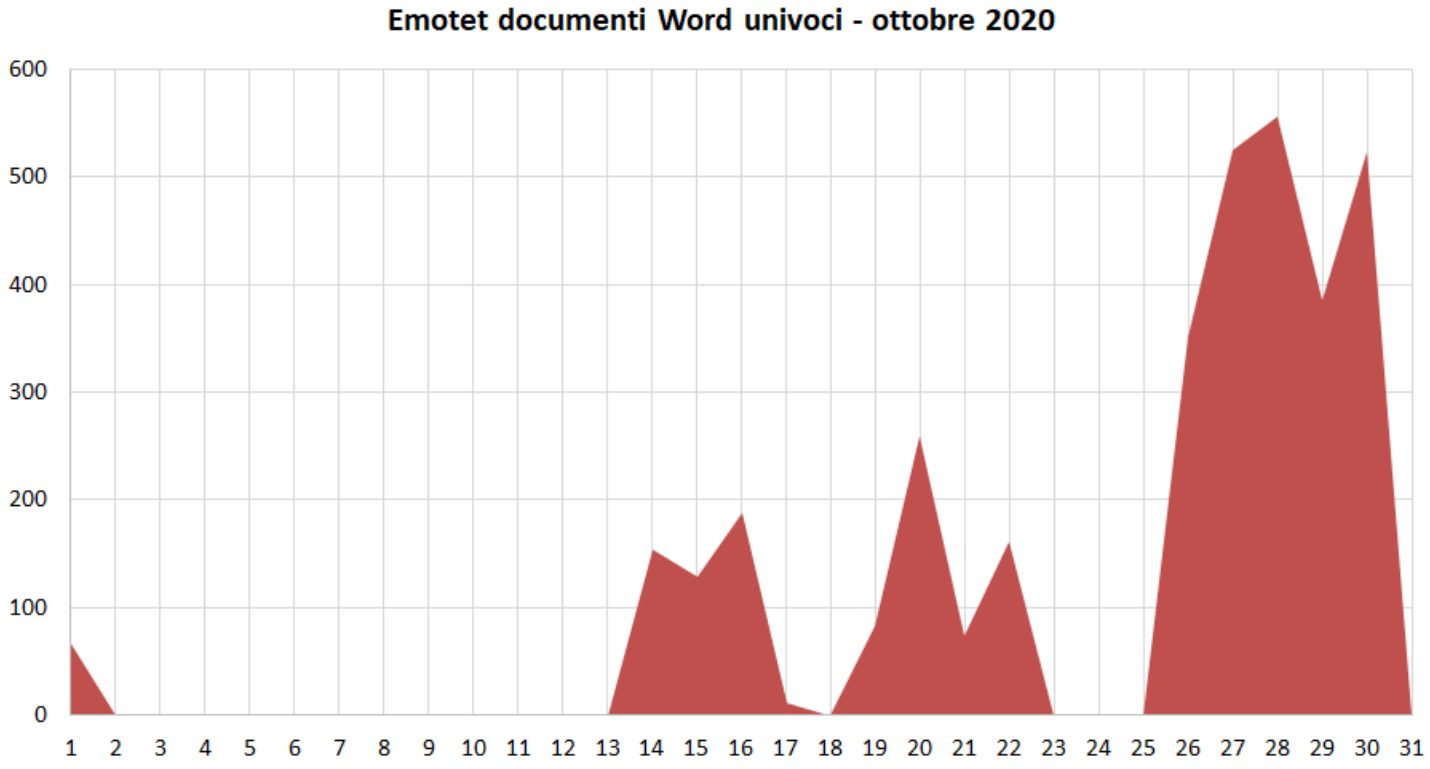
Nel mese di ottobre **Emotet** ha veicolato numerose campagne di malspam.

Nell'immagine a destra vediamo un esempio di "*reply chain*" contenente, questa volta, un link da cui viene scaricato un documento di Word infetto da Emotet.



Nel mese di ottobre Emotet ha spammato a partire dalla seconda metà del mese. Dopo una pausa di quasi 2 settimane, il 14 ottobre ha iniziato lentamente ad inviare email infette. In questo periodo si sono osservate varie modifiche e aggiustamenti ai vari stadi di Emotet. E' da lunedì 26 che Emotet ha aumentato il proprio volume di malspam toccando l'apice giovedì 28 ottobre, come è possibile vedere nel grafico sottostante.

Il numero di documenti distinti allegati alle campagne di malspam di Emotet, registra il suo picco massimo (con 556 hash univoci) giovedì 28 ottobre. A ottobre si è registrato un andamento anomalo di Emotet, dove nelle prime tre settimane gli autori si sono concentrati maggiormente nelle modifiche della parte di downloader del malware. 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, nota come "*thread hijacking*" 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 anche dal malware **Ursnif**.

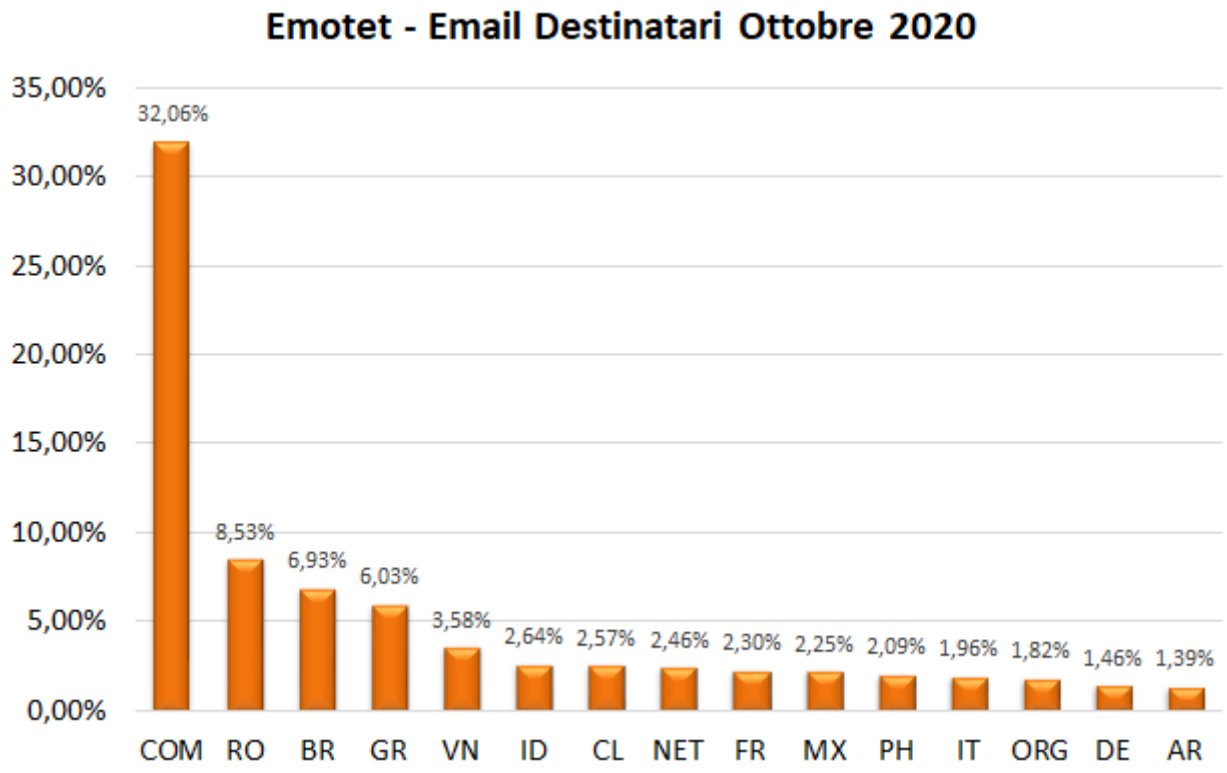
Emotet è un malware molto pericoloso, perché è in grado di infettare la rete aziendale utilizzando la tecnica dello "*spostamento laterale*", oppure attraverso un approccio indiretto rispondendo ad email interne tra colleghi della stessa azienda.

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 850.000 email monitorate dal C.R.A.M. nel mese di ottobre.

Al primo posto troviamo con oltre il 32% dei messaggi ricevuti 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 l'8.53% gli indirizzi email ".ro" della **Romania**. Il **Brasile** (.br) si posiziona al terzo posto con il 6,93% . La **Grecia** (.gr) si posiziona al quarto posto, davanti a **Francia** (.fr), **Italia** (.it) e **Germania** (.de).

L'**Italia** è stata meno colpita a ottobre da Emotet, passando dalla 6ª posizione di settembre alla 12ª posizione di ottobre, con l'1,96% delle email inviate verso indirizzi "**.it**".

Rispetto al mese di settembre sono saliti in classifica: Romania, Brasile e Grecia. Invece scendono Australia, Nuova Zelanda, Giappone e Italia, che erano stati pesantemente colpiti nel mese scorso.



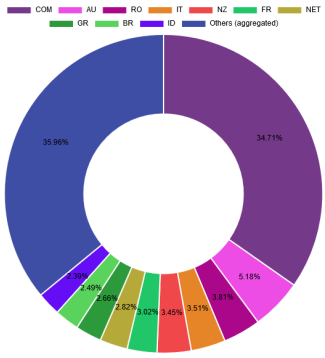
Grazie al servizio haveibeenEMOTET possiamo suddividere gli indirizzi email "abusati" da Emotet nelle seguenti tipologie:

- FAKE Sender;
- REAL Sender;
- Recipient.

Nei grafici sottostanti possiamo vedere le TOP10 da agosto a ottobre 2020, relative alle tipologie degli indirizzi email (Top Level Domain) di FAKE Sender, REAL Sender e Recipient.

TOP 10 FAKE SENDER Domain Extension compared to the total of monitored emails:

#	Domain Extension	%
1	COM	34.71 %
2	AU	5.18 %
3	RO	3.81 %
4	IT	3.51 %
5	NZ	3.45 %
6	FR	3.02 %
7	NET	2.82 %
8	GR	2.66 %
9	BR	2.49 %
10	ID	2.39 %
11	Others (aggregated)	35.96 %

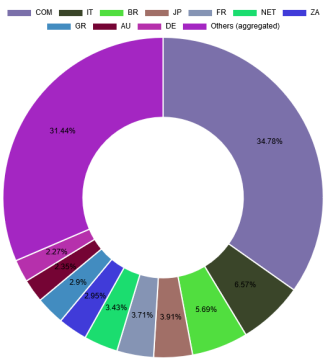


Con "FAKE Sender" Emotet cerca di impersonare il mittente del messaggio di posta, nascondendo il mittente reale attraverso un'etichetta e simulando una "reply chain", che include il corpo del messaggio rubato al mittente che sta impersonando.

Emotet per l'invio dei messaggi di posta utilizza le credenziali di autentificazione dei "REAL Sender".

TOP 10 REAL SENDER Domain Extension compared to the total of monitored emails:

#	Domain Extension	%
1	COM	34.78 %
2	IT	6.57 %
3	BR	5.69 %
4	JP	3.91 %
5	FR	3.71 %
6	NET	3.43 %
7	ZA	2.95 %
8	GR	2.9 %
9	AU	2.35 %
10	DE	2.27 %
11	Others (aggregated)	31.44 %

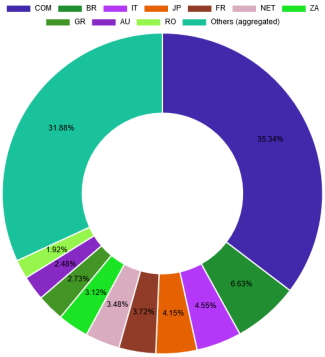


Emotet quando infetta una vittima, non si limita a rubare il corpo dei messaggi in posta in arrivo, ma ruba anche le credenziali di invio (login e password).

I Recipient di Emotet possono essere qualsiasi indirizzo email, tutti noi possiamo essere un target, ma spesso sono gli indirizzi email presenti all'interno di un thread di posta rubato alla vittima del "FAKE Sender". La tecnica è di sfruttare il collegamento tra "FAKE Sender" e Recipient, per aumentare la probabilità che il destinatario si infetti, aprendo un documento inviato da una persona che conosce.

TOP 10 RECIPIENT Domain Extension compared to the total of monitored emails:

#	Domain Extension	%
1	COM	35.34 %
2	BR	6.63 %
3	IT	4.55 %
4	JP	4.15 %
5	FR	3.72 %
6	NET	3.48 %
7	ZA	3.12 %
8	GR	2.73 %
9	AU	2.48 %
10	RO	1.92 %
11	Others (aggregated)	31.88 %



L'**Italia** sta soffrendo pesantemente gli attacchi di Emotet. Nelle TOP10, che includono il periodo tra agosto e ottobre, l'Italia si classifica rispettivamente quarta (FAKE Sender), seconda (REAL Sender) e terza (Recipient), facendo intuire che il nostro paese sia una facile terra di conquista dei cyber-criminali. Questa debacle italiana potrebbe essere dovuta ad un scarso investimento nella cyber-sicurezza delle aziende italiane. A ottobre, anche se l'Italia è stata colpita limitatamente da Emotet, alcune università e importanti aziende sono state attaccate, tra queste possiamo annoverare:

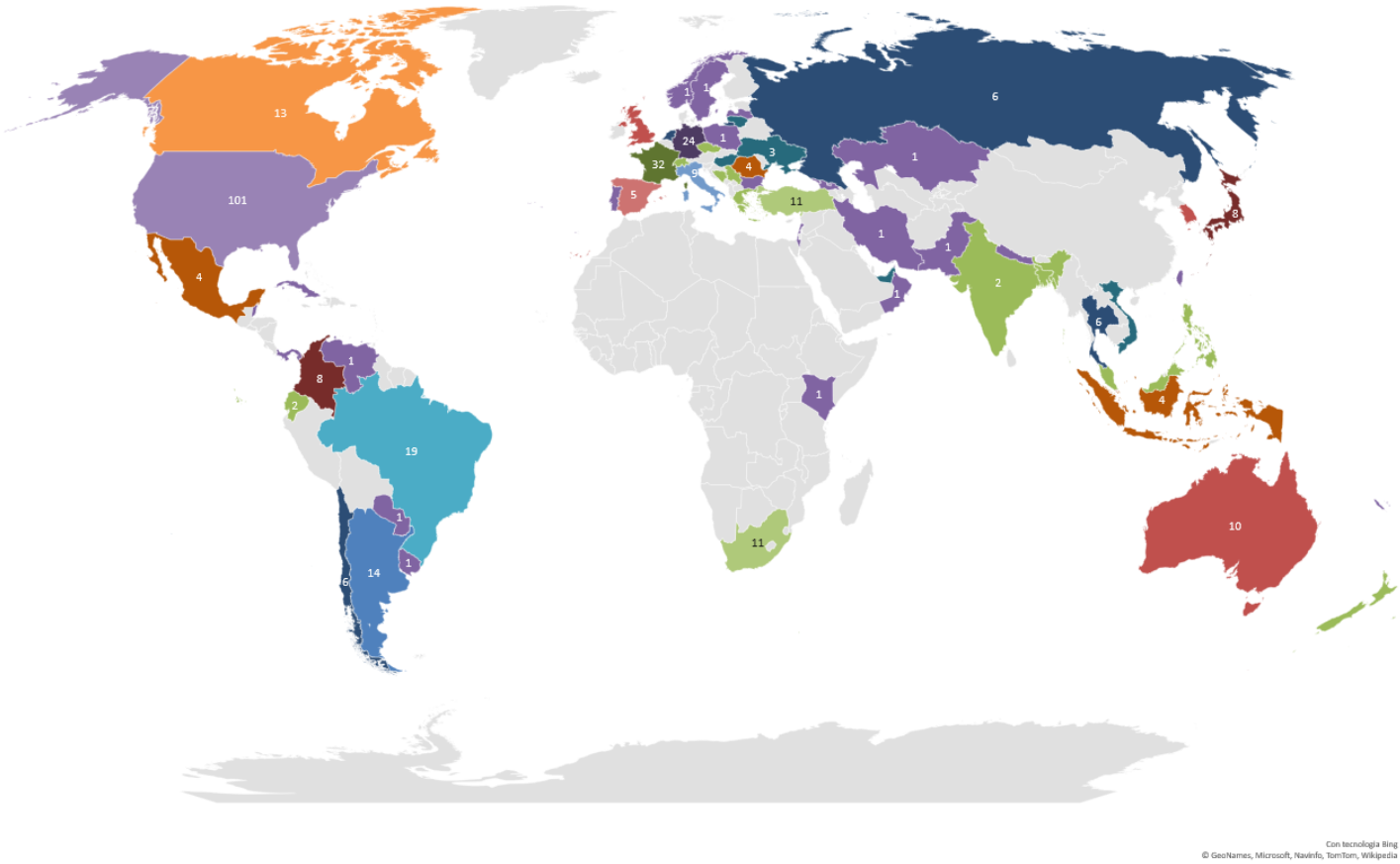
- Politecnico di Torino;
- Campari.

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 ottobre.

A ottobre Emotet si è collegato a più di **389 server C&C**. La maggior parte di questi si trovano negli **Stati Uniti d'America (101 server)**, come possiamo vedere nella tabella a fianco. Al secondo e terzo posto troviamo rispettivamente Francia e Germania. L'**Italia** si posiziona al dodicesimo posto con **9 server** di comando e controllo.

Stato	Num. Server C2
Stati Uniti	101
Francia	32
Germania	24
Brasile	29
Argentina	14
Canada	13
Sud Africa	11
Turchia	11
Australia	10
Corea del Sud	10
Gran Bretagna	10
Italia	9
Colombia	8
Giappone	8
Chile	6
Olanda	**6**
Altri Paesi	97



In Italia vi sono 9 server di comando e controllo, come possiamo vedere dalla seguente tabella:

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

IP	Città	Provider
93.147.212.206	Agrigento	Vodafone Italia S.p.A.
130.0.132.242	Milano	Vodafone Italia S.p.A.
188.219.31.12	Torino	Vodafone Italia S.p.A.
5.89.33.136	Milano	Vodafone Italia S.p.A.
2.45.176.233	Pistoia	Vodafone Italia S.p.A.
37.179.145.105	Acerra	Vodafone Italia S.p.A.
37.183.81.217	Alatri	Vodafone Italia S.p.A.
94.230.70.6	Solofra	Irpinia Net-Com SRL
37.179.204.33	Torino	Vodafone Italia S.p.A.

Ursnif

Analisi delle campagne di ottobre

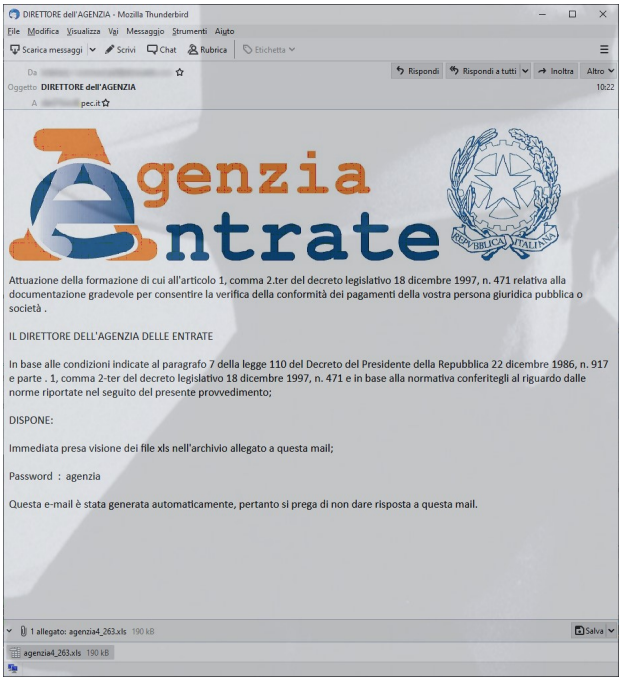
Analizziamo ora le campagne del malware bancario **Ursnif** (noto anche come **Gozi** o **IFSB**) nel mese di ottobre.

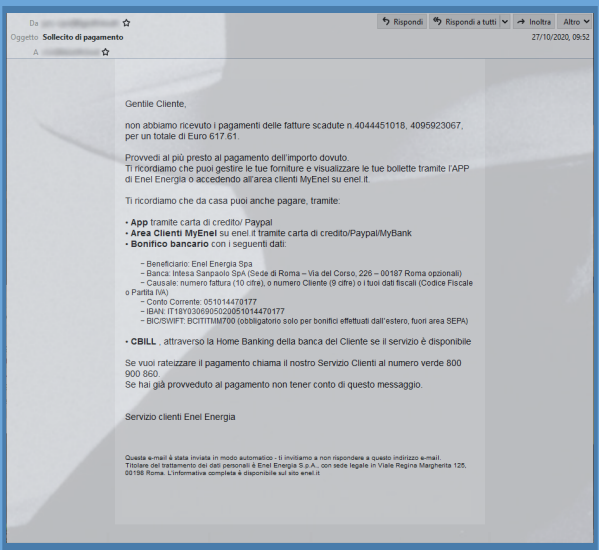
Come abbiamo visto, questo malware è uno dei più diffusi via email in Italia, a ottobre è stato veicolato attraverso 10 campagne di malspam.

Come si può vedere dalla figura a fianco, l'andamento delle campagne è stato abbastanza uniforme in tutto il mese di ottobre.

A inizio mese troviamo le prime due campagne a tema INPS. Nei giorni 6 e 7 ottobre troviamo due campagne a tema INPS e una a tema "Fattura BRT".

La campagna INPS viene riproposta ancora il 14, 19 e 20 ottobre, per poi essere sostituita il 21 ottobre dal tema "Agenzia delle Entrate". Il 27 ottobre viene sfruttato il tema "Enel Energia".



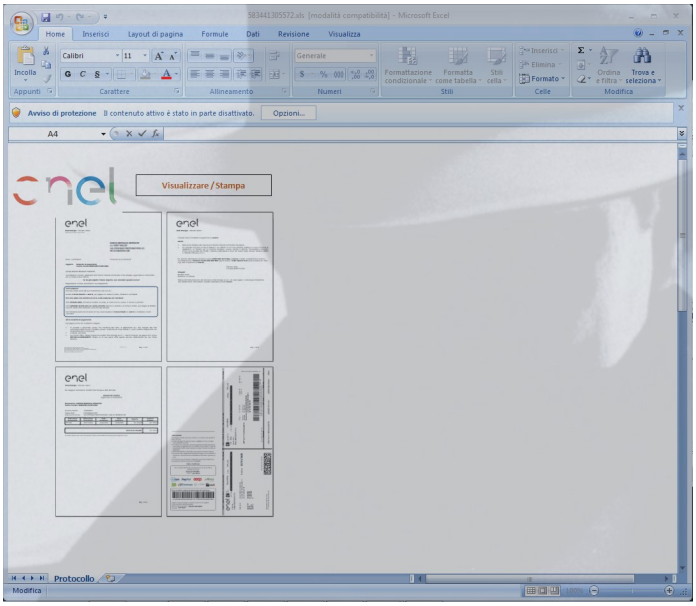


Ursnif—Campagne Malspam

01/10/2020 INPS
02/10/2020 INPS
06/10/2020 INPS
06/10/2020 Fattura BRT S.p.A.
07/10/2020 INPS
14/10/2020 INPS
19/10/2020 INPS
20/10/2020 INPS
21/10/2020 Agenzia delle Entrate
27/10/2020 Enel Energia

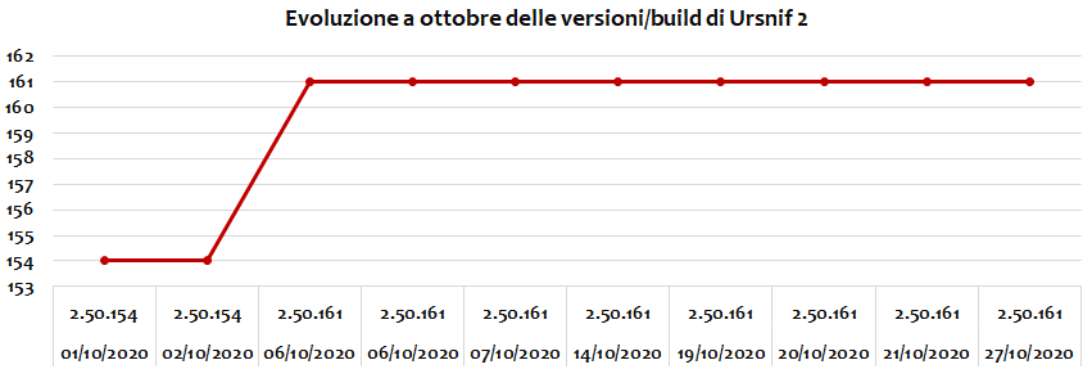
Dall'analisi delle campagne di malspam e dalle configurazioni individuate all'interno del trojan bancario Ursnif utilizzato, vi sono due gruppi distinti che stanno sfruttando questo malware a ottobre per attaccare l'utenza italiana. Il primo gruppo ha veicolato ben 8 campagne di malspam a tema INPS e Agenzia delle Entrate, invece il secondo si è limitato a sole due campagne a tema "Fattura BRT" e " Enel Energia".

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 INPS come segnalato. Il secondo invece sfrutta il tema di fatture o ordini collegati a società di spedizione come BRT (Bartolini), DHL oppure Enel Energia.



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

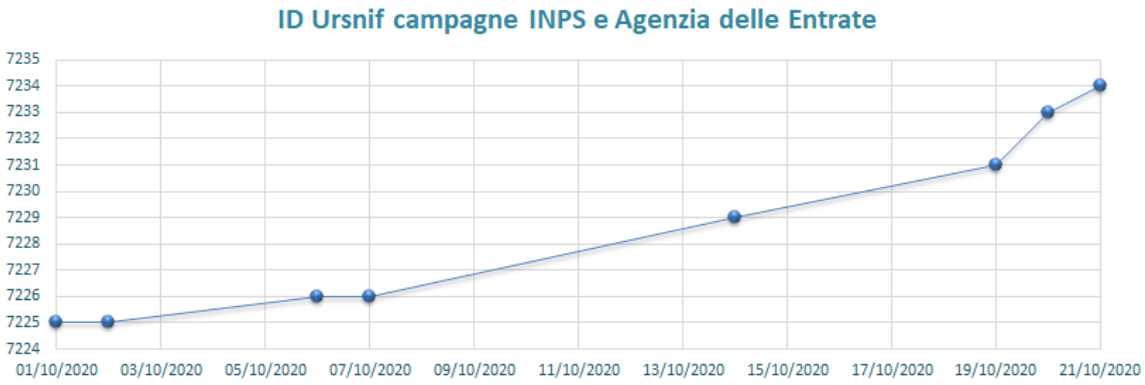
- Versione 2;
- Versione 3.



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

Nel mese di ottobre è stato rilasciato un nuovo aggiornamento del malware Ursnif, il 6 ottobre siamo passati dalla build 2.50.154 alla 2.50.161.

Nel grafico sottostante possiamo vedere come è cambiato l'ID associato al gruppo dell'Ursnif relativo alle campagne INPS e Agenzia delle Entrate nel mese di ottobre.



Nella tabella sottostante possiamo vedere l'elenco delle banche/servizi nel mirino di Ursnif nelle campagne INPS e Agenzie delle Entrate.

RelaxBanking La tua Banca di Credito Cooperativo on line	Gruppo Bancario Cooperativo Iccrea - RelaxBanking
SANFELICE 1893 BANCA POPOLARE	SANFELICE 1893 Banca Popolare
CREDEM BANCA	Credem Banca
FINECO BANK	Fineco Bank
MONTE DEI PASCHI DI SIENA BANCA DAL 1472	MONTE DEI PASCHI DI SIENA
PayPal	PayPal
UniCredit	UniCredit
nexi	Nexi
Deutsche Bank	Deutsche Bank
Volksbank	Volksbank - direct b@anking
Volksbank	Volksbank - CoB@ web
amazon seller central	Amazon seller central

MONTE DEI PASCHI DI SIENA - aziendaonline

BANCA PASSADORE & C.

Posteitaliane - BPIOL

Banca Sella

Banca Popolare di Sondrio - SCRIGNOmultibanca

Banca di Cividale

Banca di Cividale - Conto Green

Banca Profilo

CREDIT AGRICOLE - CariParma

CREDIT AGRICOLE - Friuladria

BPER Banca

Banca Mediolanum

BANCA WIDIBA

FIDEURAM

Poste italiane

CABEL

Poste italiane

BNL - Business

INTESA SANPAOLO - INBIZ

BANCA mediolanum - CEDACRI

Deutsche Bank

Deutsche Bank - Quercia

BNL Banking

BANCA CARIGE

BANCO BPM

UBI BANCA

Desio Web Banking - CEDACRI

Banco di Sardegna

INBANK

Poste italiane

Ransomware

Ottobre 2020—ITALIA

Continuano gli attacchi ransomware utilizzando differenti vettori d'infezione.

Questo mese registriamo un aumento degli attacchi ransomware rispetto al mese scorso.

La nostra telemetria ha registrato gli attacchi dei seguenti ransomware:

- **Dharma;**
- **Phobos;**
- **ShivaGood.**

I ransomware identificati a ottobre derivano da attacchi attraverso il desktop remoto (RDP) mirati verso aziende italiane.

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

Dharma e **Phobos** sono stati molto attivi a ottobre con numerosi attacchi via RDP, di seguito riportiamo la lista delle estensioni aggiunte ai file cifrati:

- .BLM
- .ROGER
- .BK
- .ABKIR
- .EKING

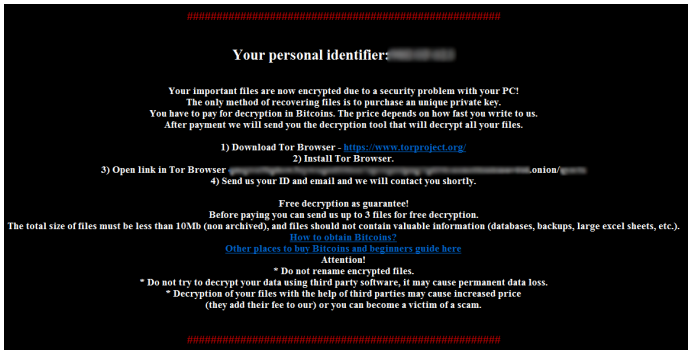
ShivaGood non è un ransomware nuovo, le prime versione di questo ransomware risalgono al 2019.

L'attacco in questione è avvenuto via RDP nel tardo pomeriggio di sabato 24 ottobre, con la seguente cronologia di operazioni:

1. **2020-10-24 18:37:50** tentativo di disinstallazione dell'anti-virus;
2. **2020-10-25 dalle 01:14 alle 04:07** in questo arco temporale vengono eseguite diverse istanze del ransomware ShivaGood con i seguenti nomi: FROST.EXE, FROST_1.EXE, FROST(6).EXE, FROST(5).EXE, FROS.EXE.

Il cyber-criminale ha eseguito numerose volte il ransomware, perché il sistema anti-ransomware di VirIT eXplorer PRO bloccava la cifratura dei file.

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



Gli accessi remoti (RDP) sono avvenuti a partire dal 19 ottobre , dove il cyber-criminale si è collegato con cadenza quasi giornaliera fino al 25 ottobre, utilizzando i seguenti account:

- Administrator;
- Sys.

La password dell'account Administrator molto probabilmente è stata individuata con un attacco brute-force. Il cyber-criminali ha utilizzato entrambi gli account per eseguire le diverse istanze del ransomware tra il 24 e 25 ottobre.

L'IP del cyber-criminale è stato geo-localizzato in Russia.

Nel mese di settembre diverse testate giornalistiche e media avevano dato notizia di un attacco informatico verso **Luxottica S.p.A.,** che aveva portato al blocco della produzione per l'intera giornata del 21 settembre.

Il 18 ottobre l'attacco informatico a **Luxottica S.p.A.** è stato rivendicato dal cyber-gruppo criminale **NEFILIM** attraverso un post pubblicato nel proprio portale "Corporate Leaks" nel dark web.

Nella rivendicazione dell'incidente capitato a Luxottica, i cyber-criminali forniscono come prova che l'attacco sia riuscito una prima parte dei dati esfiltrati:

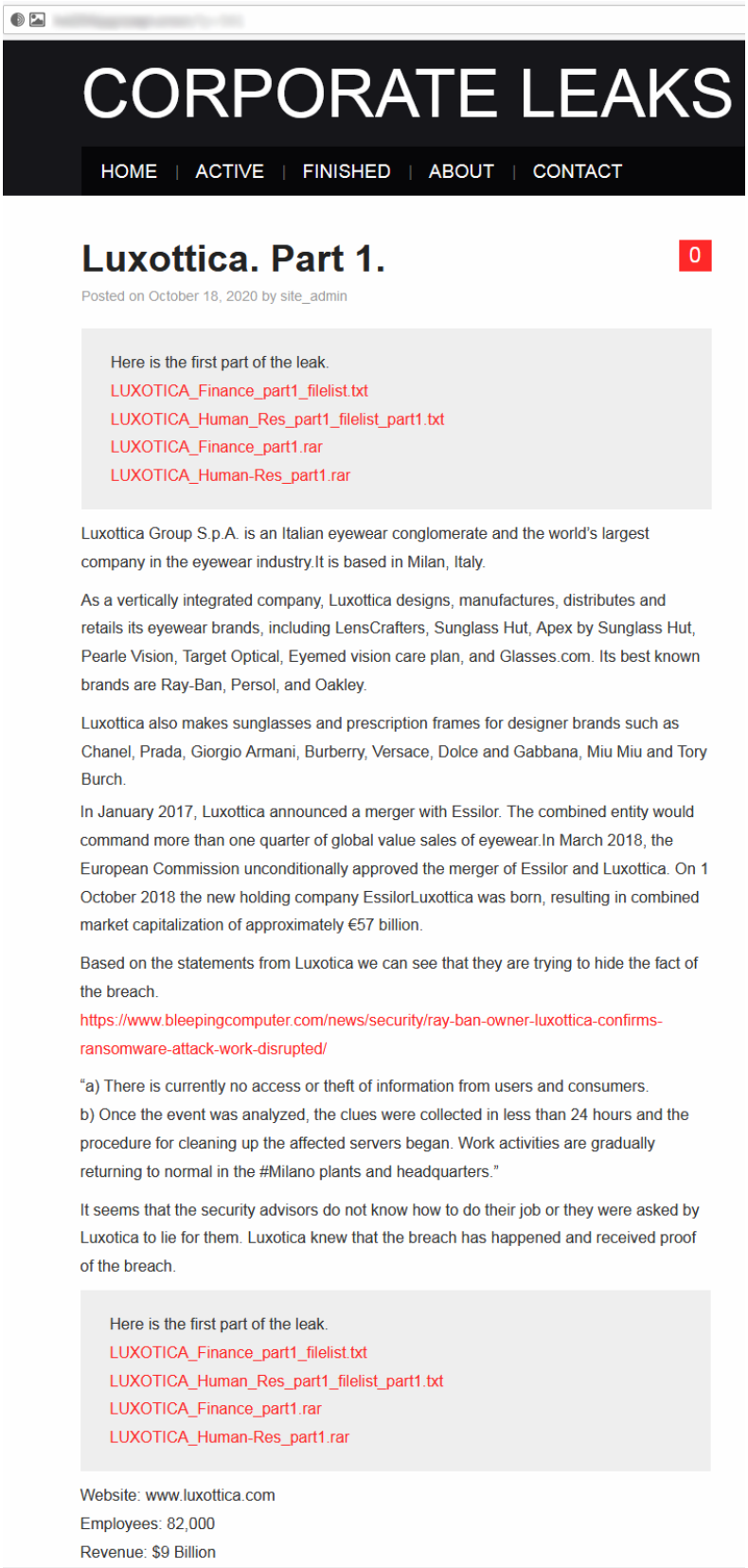
- Finance_part1.rar (1,8 GB)
- Human Res_part1.rar (2 GB)

Il 30 ottobre i cyber-criminali hanno pubblicato una seconda parte:

- LUXOTICA_Finance_part_2.rar (18 GB)

Il 7 novembre sono state pubblicate ulteriori parti (3, 4, 5 and other) del leak a Luxottica:

- 003_LUXOTICA_Human_Resource _part_3.rar (10 GB)
- LUXOTICA_banking_part_4.rar (2,2 GB)
- LUXOTICA_e_com_part_5.rar (6,3 GB)
- LUXOTICA_other_part_8.rar (17,2 GB)



CORPORATE LEAKS

HOME | ACTIVE | FINISHED | ABOUT | CONTACT

Luxottica. Part 1.

0

Posted on October 18, 2020 by site_admin

Here is the first part of the leak.
LUXOTICA_Finance_part1_filelist.txt
LUXOTICA_Human_Res_part1_filelist_part1.txt
LUXOTICA_Finance_part1.rar
LUXOTICA_Human-Res_part1.rar

Luxottica Group S.p.A. is an Italian eyewear conglomerate and the world's largest company in the eyewear industry.It is based in Milan, Italy.

As a vertically integrated company, Luxottica designs, manufactures, distributes and retails its eyewear brands, including LensCrafters, Sunglass Hut, Apex by Sunglass Hut, Pearle Vision, Target Optical, Eyemed vision care plan, and Glasses.com. Its best known brands are Ray-Ban, Persol, and Oakley.

Luxottica also makes sunglasses and prescription frames for designer brands such as Chanel, Prada, Giorgio Armani, Burberry, Versace, Dolce and Gabbana, Miu Miu and Tory Burch.

In January 2017, Luxottica announced a merger with Essilor. The combined entity would command more than one quarter of global value sales of eyewear.In March 2018, the European Commission unconditionally approved the merger of Essilor and Luxottica. On 1 October 2018 the new holding company EssilorLuxottica was born, resulting in combined market capitalization of approximately €57 billion.

Based on the statements from Luxotica we can see that they are trying to hide the fact of the breach.
https://www.bleepingcomputer.com/news/security/ray-ban-owner-luxottica-confirms-ransomware-attack-work-disrupted/

"a) There is currently no access or theft of information from users and consumers.
b) Once the event was analyzed, the clues were collected in less than 24 hours and the procedure for cleaning up the affected servers began. Work activities are gradually returning to normal in the #Milano plants and headquarters."

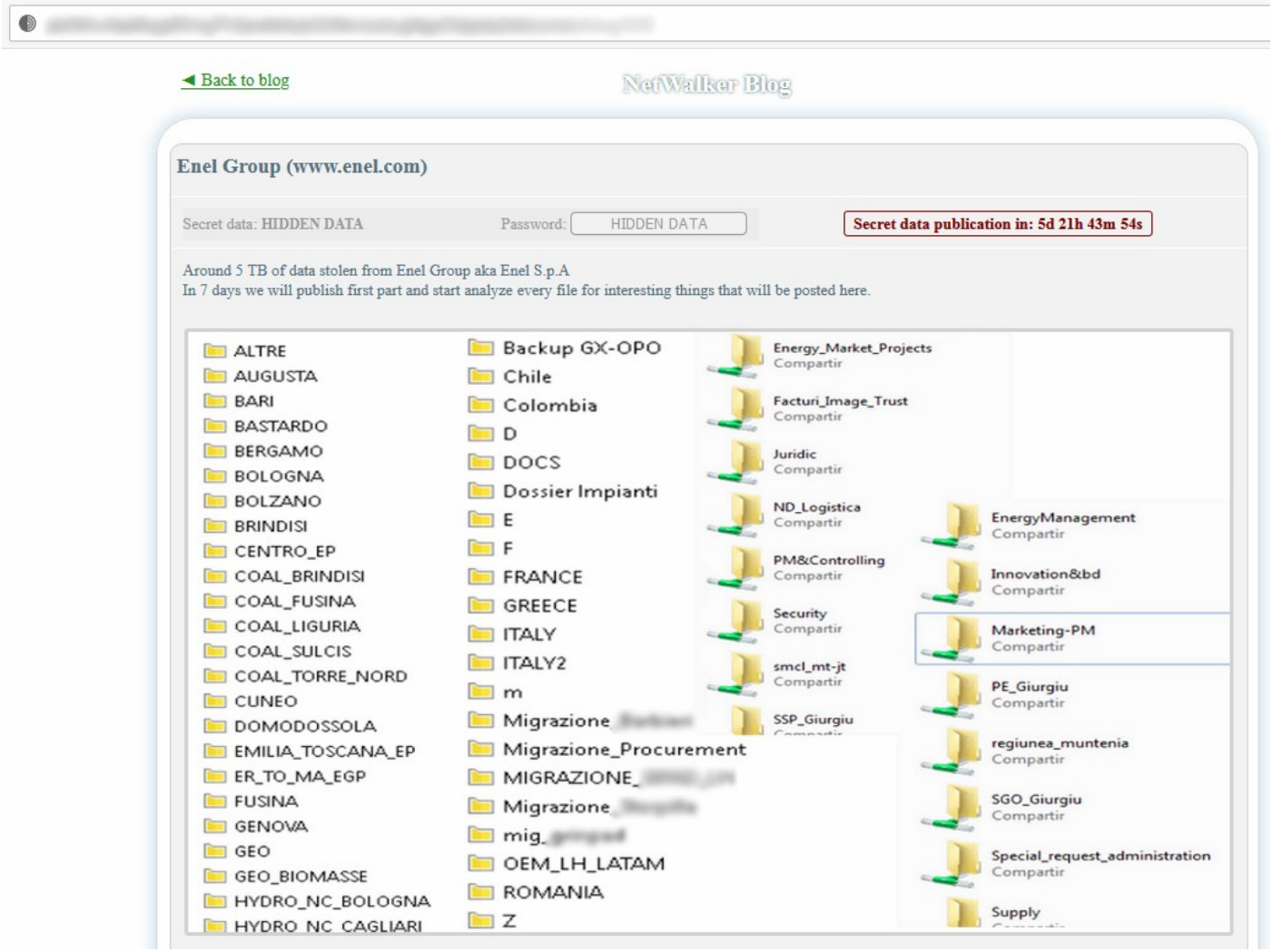
It seems that the security advisors do not know how to do their job or they were asked by Luxotica to lie for them. Luxotica knew that the breach has happened and received proof of the breach.

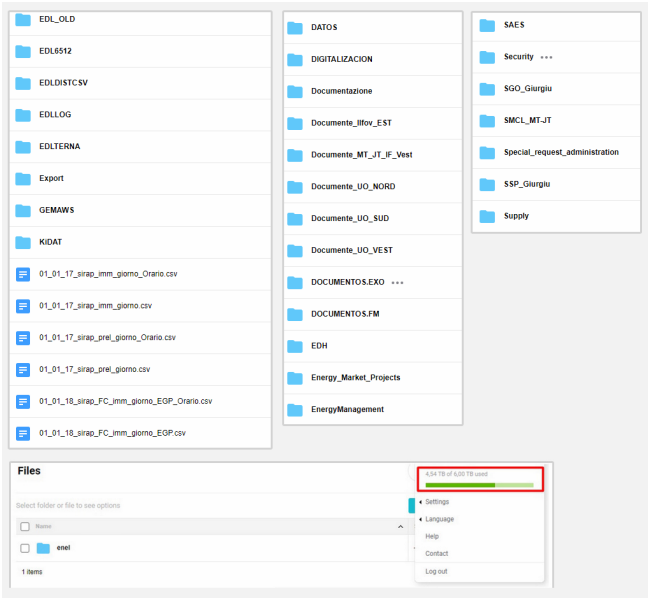
Here is the first part of the leak.
LUXOTICA_Finance_part1_filelist.txt
LUXOTICA_Human_Res_part1_filelist_part1.txt
LUXOTICA_Finance_part1.rar
LUXOTICA_Human-Res_part1.rar

Website: www.luxottica.com
Employees: 82,000
Revenue: $9 Billion

Il 27 ottobre la società **ENEL S.p.A.** è stata colpita da un attacco ransomware con esfiltrazione di dati.

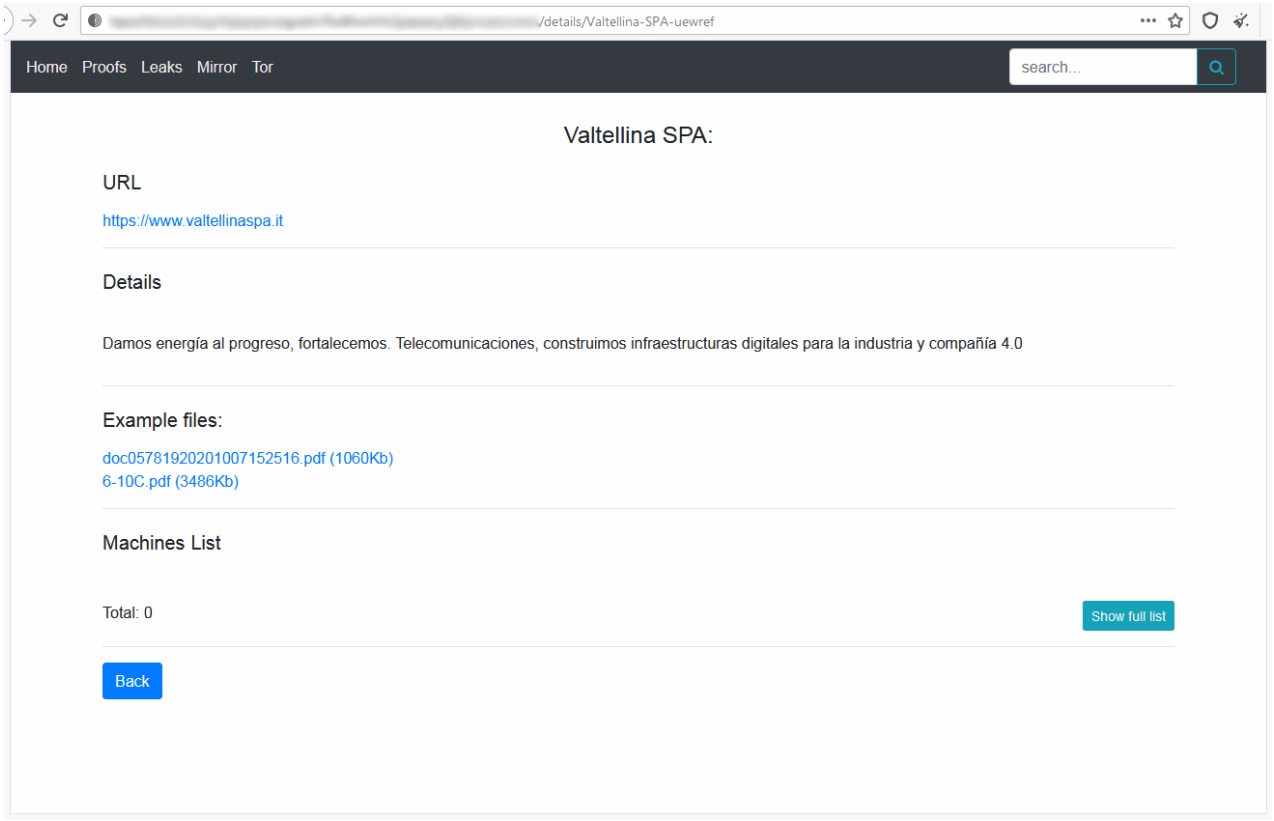
A darne notizia è stato il gruppo di cyber-criminali di **NetWalker** attraverso un post nel proprio blog nel dark web. Secondo NetWalker avrebbero esfiltrato circa 5 TB di dati da Enel S.p.a., come possiamo vedere dalle seguenti immagini:





Il 28 ottobre un'altra società italiana la **Valtellina S.p.A.** è stata colpita da un attacco ransomware con esfiltrazione di dati.

A darne notizia questa volta è stato il gruppo di cyber-criminali **DoppelPaymer** attraverso un post nel proprio portale nel dark web.



Prevalenza

Ottobre 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.

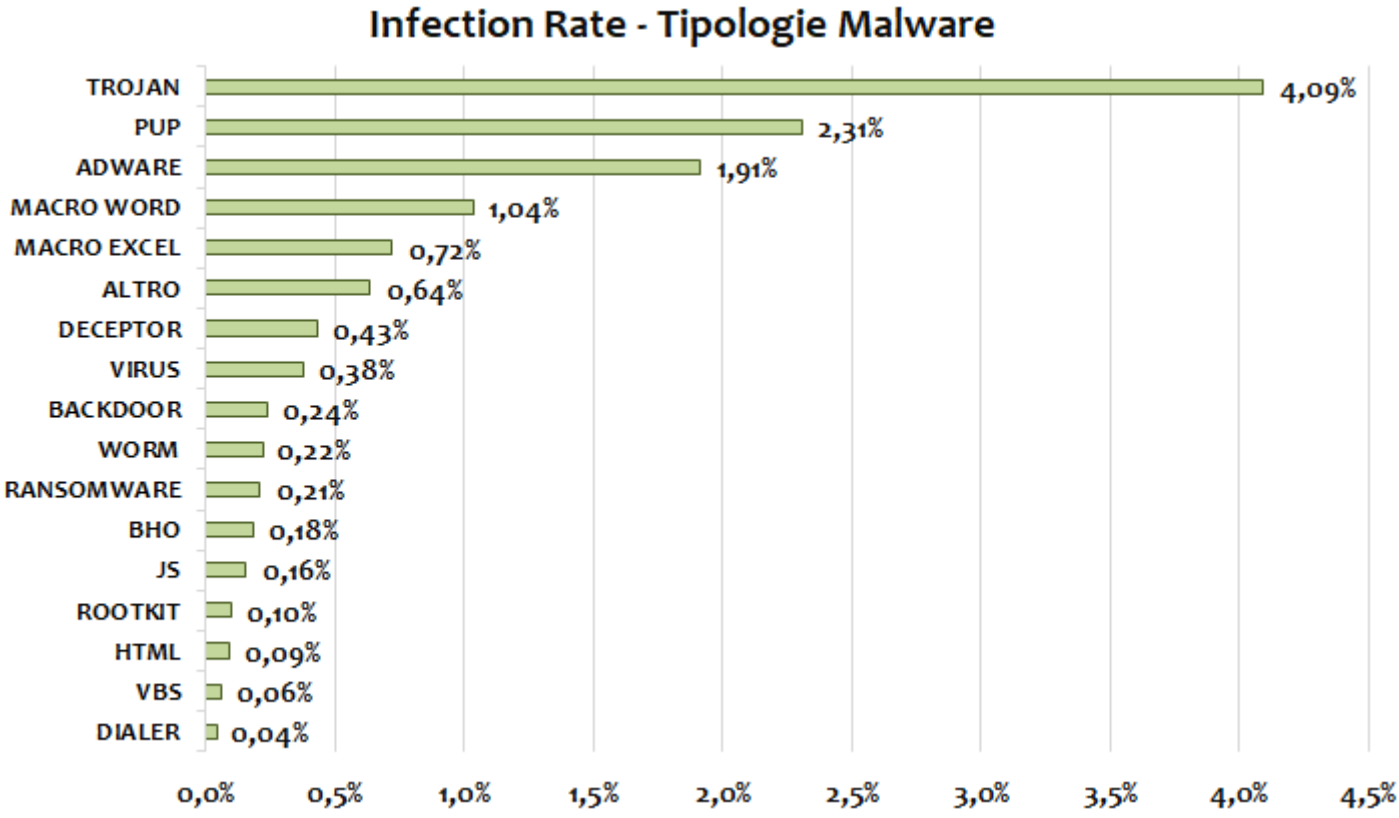
Vediamo ora i dati relativi alla prevalenza dei malware registrati dal C.R.A.M. di TG Soft nel mese di ottobre. Per prevalenza si intende l'incidenza che i malware hanno in un determinato periodo. Il valore calcolato si chiama "rate di infezione".

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 4,09%. Secondo posto confermato per i **PUP** , con una percentuale del 2,31%. Terzo gradino del podio per la categoria **Adware** con l'1,91%.

Dalla 4ª alla 6ª posizione troviamo i **MACRO WORD**, seguiti dalle **MACRO di EXCEL** e dal gruppo generico denominato **Altro** (che include le macro di Office generiche). Si attestano in 11ª posizione i **Ransomware** con lo 0,21%. 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.).

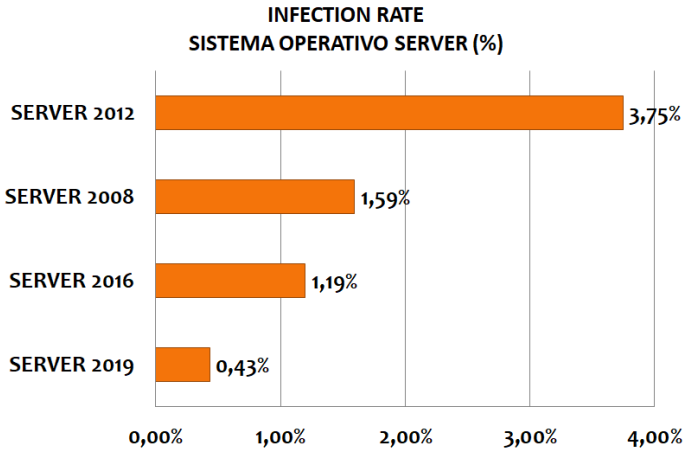


Andiamo ora ad analizzare la prevalenza delle infezioni del mese di ottobre in base ai sistemi operativi suddivisi tra sistemi Server e Client.

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 0,43% contro 3,75%.

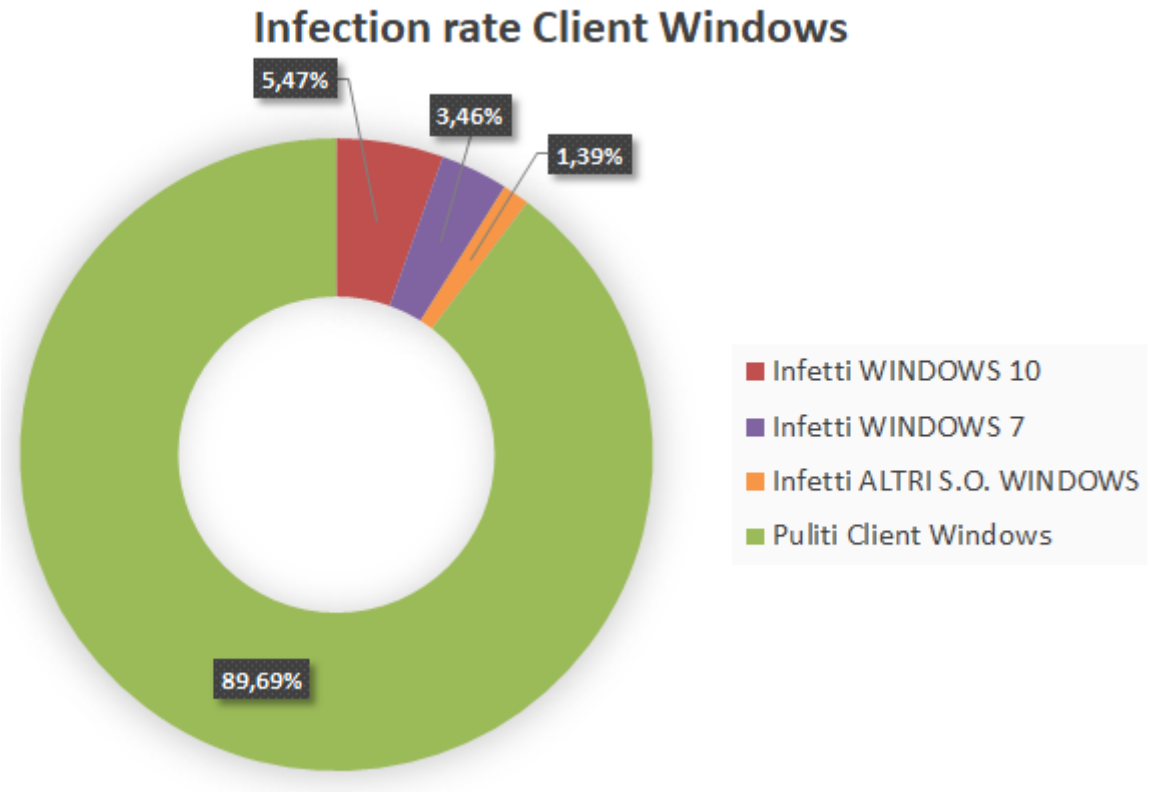
Nelle statistiche relative alla prevalenza delle infezioni dei computer client nel mese di ottobre abbiamo riscontrato che il **10,31%** dei terminali è stato infettato o ha subito un attacco. Questo dato



indica che **10 computer su 100** sono stati colpiti da malware nel mese di ottobre.

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

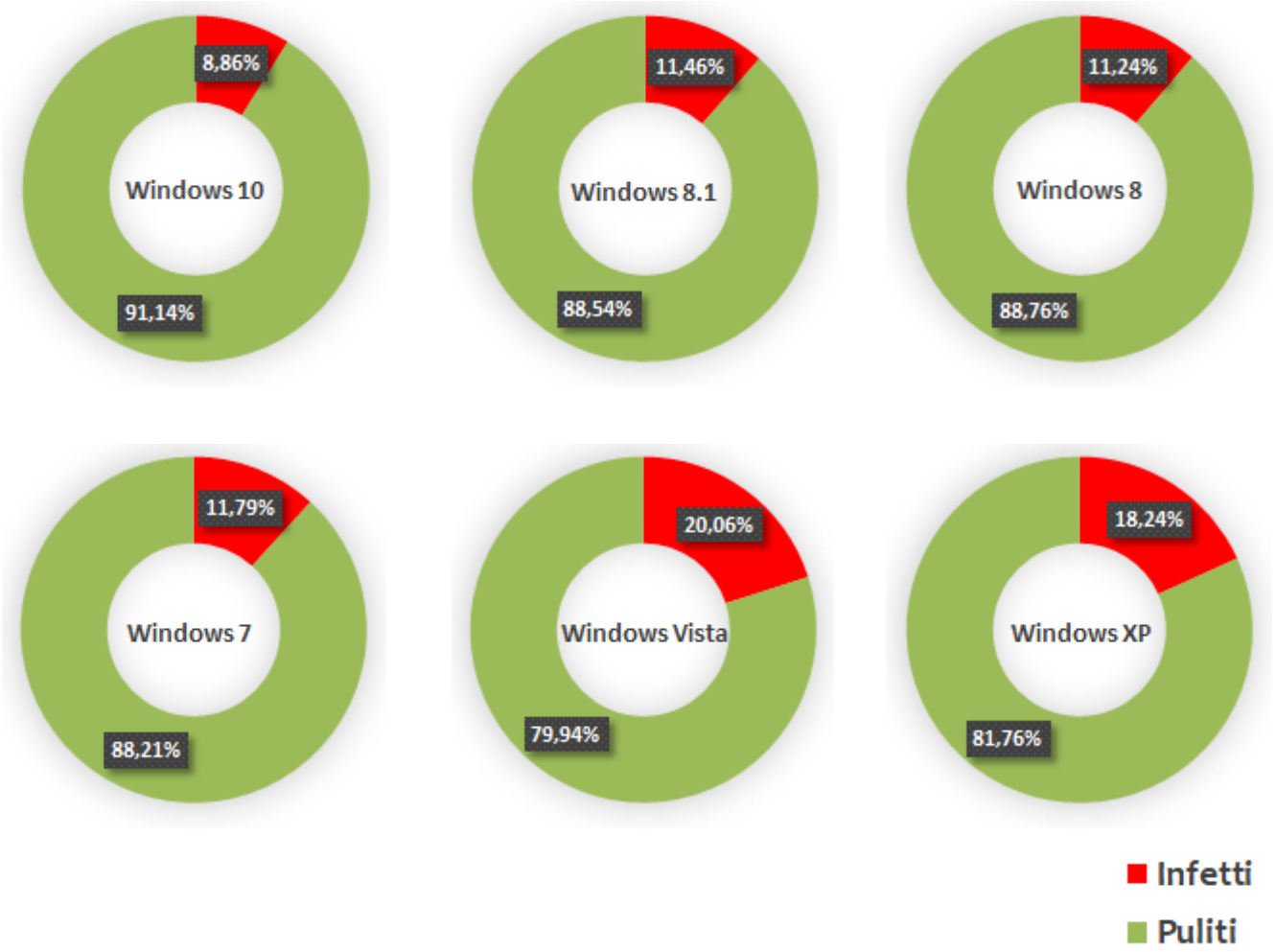
- 61,67% client con Windows 10
- 29,32% client con Windows 7
- 9,01% client con altri s.o. Windows



Windows 10 e **Windows 7** coprono più del 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 ?

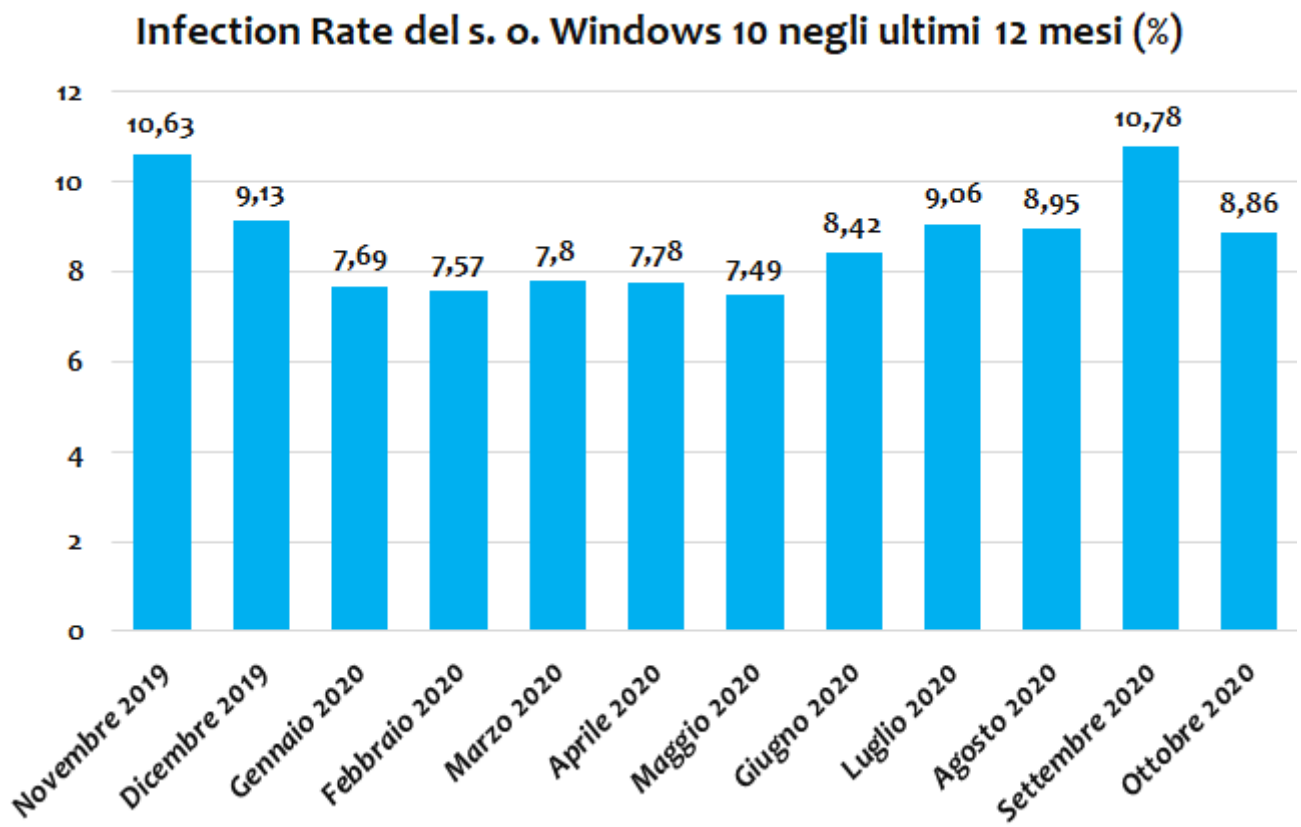
Per rispondere a questa domanda dobbiamo calcolare la prevalenza d'infezione sul medesimo sistema operativo. Prendendo ad esempio Windows 10, si può notare che il rate di infezione tra tutte le macchine ove è installato Windows 10 che ha subito un attacco informatico è del 8,86% . Con questo calcolo 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 più del 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 stato settembre 2020. In quel periodo si è avuto in Italia una massiva diffusione di campagne malware atte a distribuire il trojan Emotet. Negli ultimi 12 mesi Emotet si è diffuso da novembre 2019 a fino a metà febbraio 2020, per poi riprendere la sua attività dal mese di luglio 2020. Nel mese di ottobre registriamo un leggere incremento dei cluster di malware, ma un decremento del numero delle infezioni rispetto al mese scorso. Questo calo di infezioni è dovuto principalmente alla forte diminuzione delle campagne di malspam di Emotet registrate in Italia.



TG Soft
Cyber Security Specialist
www.tgsoft.it