Cyber-Threat Report

Settembre 2020

TG Soft
Cyber Security Specialist
www.tgsoft.it

Settembre 2020

TG Soft
Cyber-Threat Report

Notizie di rilievo:

haveibeenEMOTET

Panorama delle minacce in Italia a settembre

Sommario:

Nel mese di settembre si è riscontrato un incremento degli attacchi informatici ed una leggera crescita del numero dei cluster di malware rispetto al mese di agosto.

A settembre **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 settembre abbiamo una diversificazione degli attacchi malware. Nella settimana successiva vi è stato un calo di campagne malspam, per riprendere in modo prepotente dalla metà fino alla fine del mese.

Ursnif è stato poco attivo, riscontriamo un certo movimento solamente nella terza decade del mese. Nuovi password stealer/RAT si sono affacciati nel panorama italiano: **Mekotio**, **Matiex** e **XpertRat**. Sono continuati gli attacchi RDP che hanno veicolato i ransomware **LockBit, Makop** e **Phobos**. E' tornato **Avaddon** collegato all'Agenzia delle Entrate.

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.

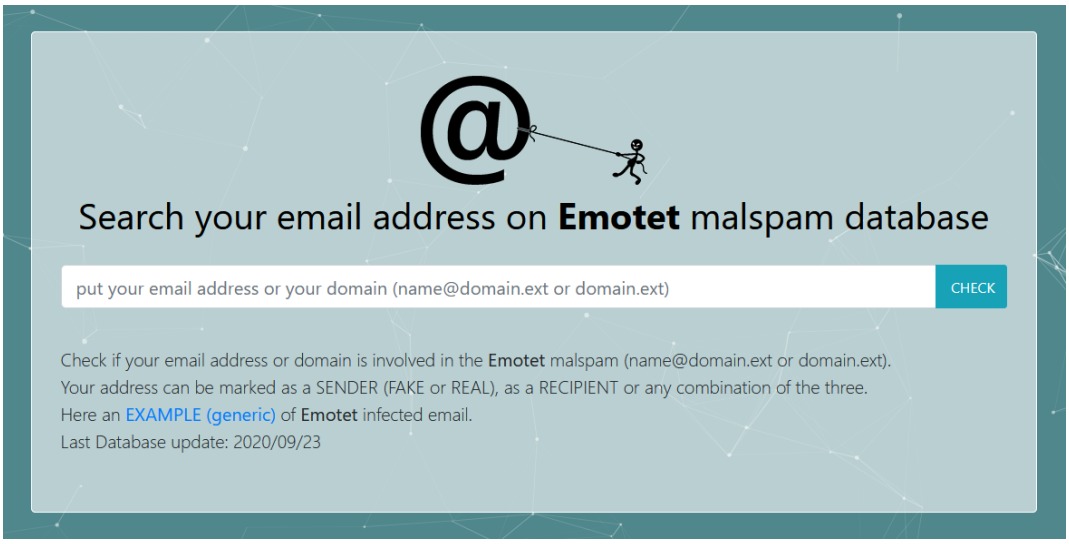
L'indice che misura lo stato della Cyber-Security è l'Infection Rate (IR), che è la percentuale degli utenti dell'anti-virus Vir.IT eXplorer che hanno incontrato una minaccia che sia stata segnalata al C.R.A.M. di TG Soft.

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

haveibeenEMOTET



Il 1° Ottobre 2020 il **C.R.A.M.** di **TG Soft** ha sviluppato e reso disponibile al pubblico il portale haveibeenEMOTET (https://www.haveibeenemotet.com) che permette, in maniera totalmente gratuita, di verificare se un indirizzo di posta elettronica o un dominio è stato coinvolto nelle attività di MalSpam del Malware Emotet.

Grazie al sistema proprietario di Threat Intelligence interamente sviluppato ad hoc e ad una rete di honeypot il C.R.A.M. di TG Soft è in grado di monitorare e poi bloccare le attività di MalSpam in uscita svolte dal Malware Emotet nelle Honeypot ed estrarne quindi le informazioni.

Effettuando la ricerca attraverso il portale haveibeenEMOTET l'indirizzo email o il dominio può essere segnalato come:

⇒ **Mittente Fake (Fake Sender)** -> Le email non vengono inviate dal tuo account, ma il tuo indirizzo email è utilizzato come etichetta per nascondere il Mittente Reale, questo indica che potresti essere o essere stato infetto. Le tue email/contatti potrebbero essere stati rubati. E' necessario procedere ad un cambio delle password ed effettuare una scansione AntiVirus*.

⇒ **Mittente Reale (Real Sender)** -> Il reale account email utilizzato dalla Botnet di Emotet per effettuare l'invio effettivo dello SPAM, questo indica che la password del tuo account di posta elettronica è stata compromessa e che potresti essere o essere stato infetto. Le tue email ed/o i tuoi contatti potrebbero essere stati rubati. E' necessario procedere ad un cambio delle password ed effettuare una scansione AntiVirus*.

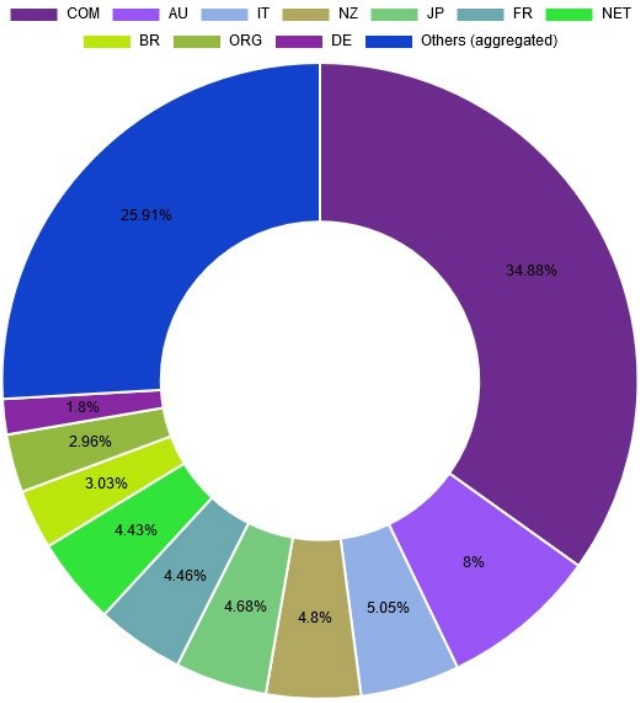
⇒ **Destinatario (Recipient)** -> Questo indica che l'indirizzo email/dominio hanno ricevuto e-mail di MalSpam da Emotet, è necessario quindi prestare massima attenzione alle email ricevute anche da contatti conosciuti. Non è superfluo effettuare un controllo AntiVirus oltre quello abitualmente in uso*.

* Vir.IT eXplorer Lite è disponibile al bisogno, GRATUITAMENTE, liberamente utilizzabile sia in ambito privato come anche aziendale, interoperabile con qualsiasi altro anti-virus o Internet Security già presente nel computer senza conflittualità e senza necessità di sua disinstallazione.

Nel portale sono disponibili inoltre le statistiche (https://www.haveibeenemotet.com/stats.php) sulle estensioni dominio più colpite, è possibile pertanto vedere una panoramica generalizzata di quali siano le estensioni dei domini più colpiti, da cui i paesi maggiormente presi di mira da Emotet:

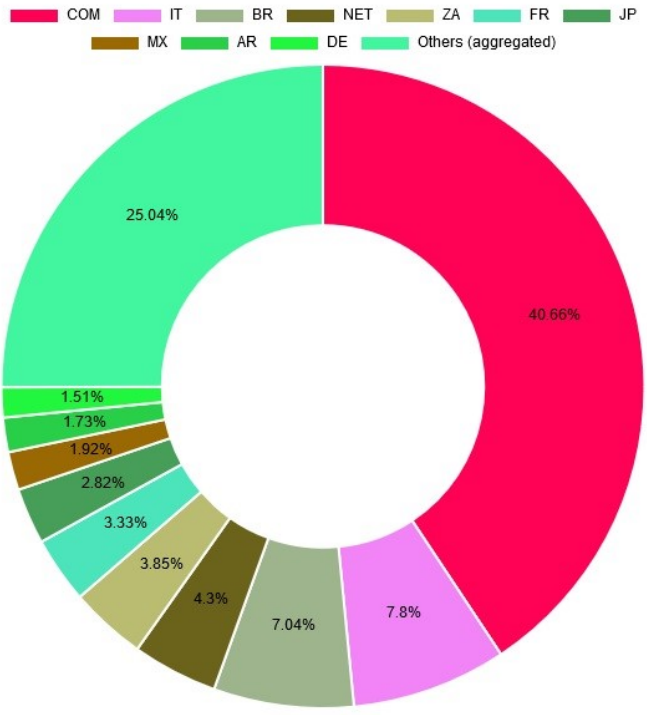
TOP 10 FAKE SENDER Domain Extension compared to the total of monitored emails:

#	Domain Extension	%
1	COM	34.88 %
2	AU	8 %
3	IT	5.05 %
4	NZ	4.8 %
5	JP	4.68 %
6	FR	4.46 %
7	NET	4.43 %
8	BR	3.03 %
9	ORG	2.96 %
10	DE	1.8 %
11	Others (aggregated)	25.91 %



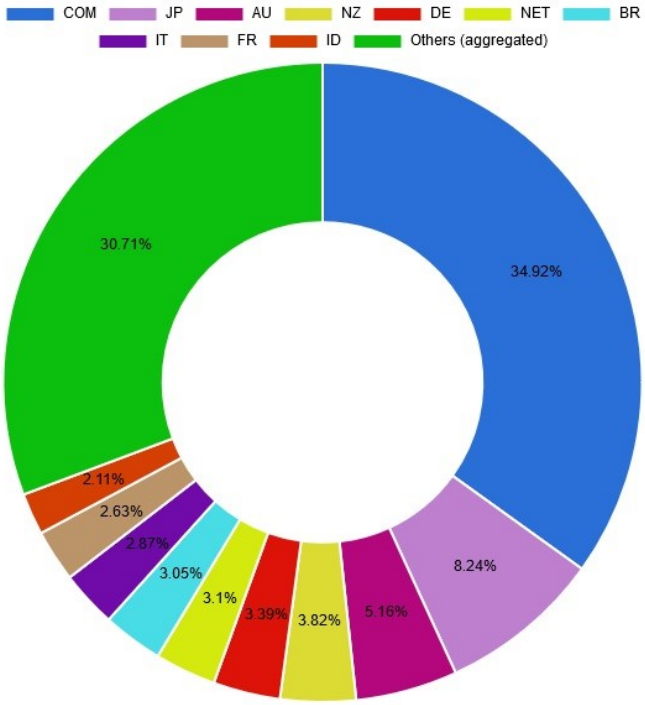
TOP 10 REAL SENDER Domain Extension compared to the total of monitored emails:

#	Domain Extension	%
1	COM	40.66 %
2	IT	7.8 %
3	BR	7.04 %
4	NET	4.3 %
5	ZA	3.85 %
6	FR	3.33 %
7	JP	2.82 %
8	MX	1.92 %
9	AR	1.73 %
10	DE	1.51 %
11	Others (aggregated)	25.04 %



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

#	Domain Extension	%
1	COM	34.92 %
2	JP	8.24 %
3	AU	5.16 %
4	NZ	3.82 %
5	DE	3.39 %
6	NET	3.1 %
7	BR	3.05 %
8	IT	2.87 %
9	FR	2.63 %
10	ID	2.11 %
11	Others (aggregated)	30.71 %

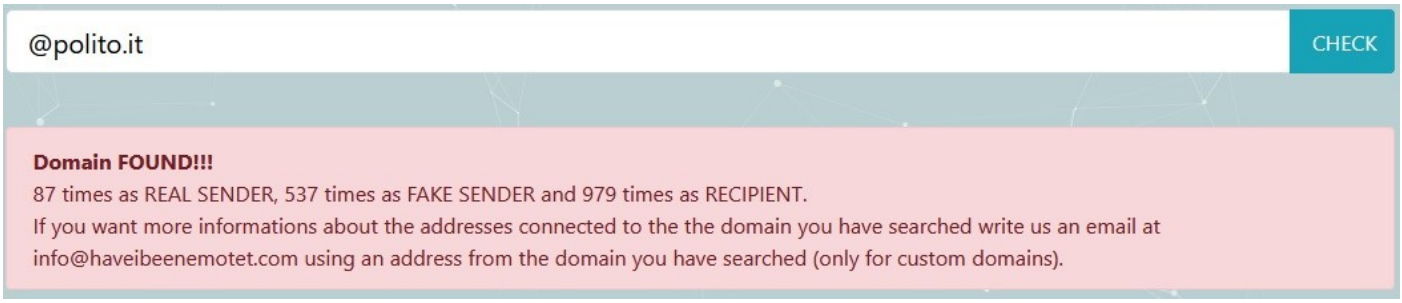


Come si può notare dai grafici l'estensione dominio che rappresenta l'**Italia** ".IT" è presente nella TOP 10 di tutte e tre le classifiche (Fake Sender, Real Sender, Recipient). In particolare si trova in **seconda posizione** nella classifica dei REAL SENDER superata solo dall'estensione dominio generica ".COM", e seguita dal Brasile (.BR).

Questi grafici fanno riflettere sullo stato della Cyber Security in Italia, evidenziando una situazione indice di scarsa attività di monitoraggio e di esecuzione di quelle che sono le "best practice" informatiche anche quelle più basilari, come ad esempio eseguire il cambio delle password regolarmente.

Possiamo vedere nelle prossime immagini che anche gli enti governativi non sono esenti dall'essere colpiti dalle attività malevole di Emotet.

Politecnico di Torino



CNR (Consiglio Nazionale delle Ricerche)

@cnr.it CHECK

Domain FOUND!!!
47 times as REAL SENDER, 11 times as FAKE SENDER and 103 times as RECIPIENT.
If you want more informations about the addresses connected to the the domain you have searched write us an email at info@haveibeenemotet.com using an address from the domain you have searched (only for custom domains).

Sapienza Università di Roma

@uniroma1.it CHECK

Domain FOUND!!!
66 times as REAL SENDER, 44 times as FAKE SENDER and 124 times as RECIPIENT.
If you want more informations about the addresses connected to the the domain you have searched write us an email at info@haveibeenemotet.com using an address from the domain you have searched (only for custom domains).

Esercito italiano

@esercito.difesa.it CHECK

Domain FOUND!!!
0 times as REAL SENDER, 4 times as FAKE SENDER and 2 times as RECIPIENT.
If you want more informations about the addresses connected to the the domain you have searched write us an email at info@haveibeenemotet.com using an address from the domain you have searched (only for custom domains).

Regione Lombardia

@regione.lombardia.it CHECK

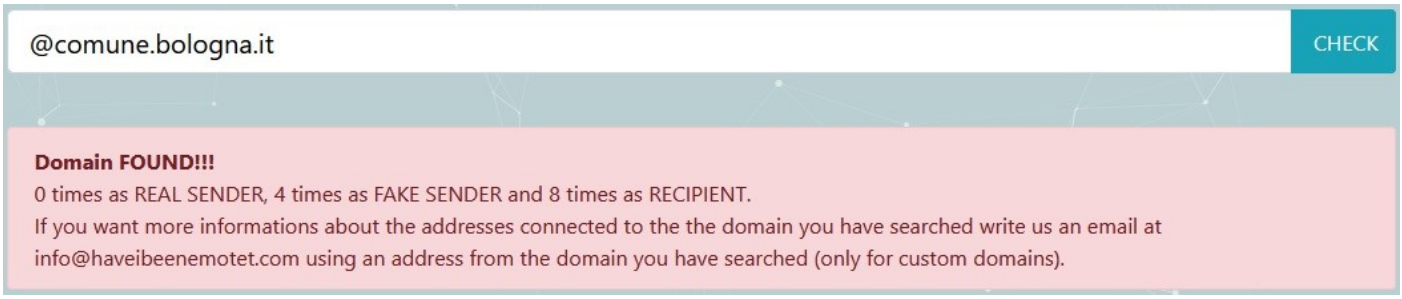
Domain FOUND!!!
0 times as REAL SENDER, 2 times as FAKE SENDER and 8 times as RECIPIENT.
If you want more informations about the addresses connected to the the domain you have searched write us an email at info@haveibeenemotet.com using an address from the domain you have searched (only for custom domains).

Università di Milano

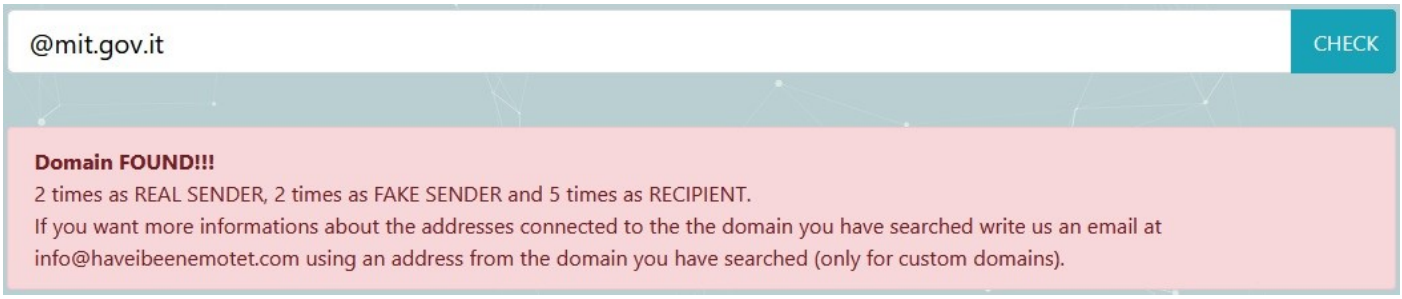
@unimi.it CHECK

Domain FOUND!!!
24 times as REAL SENDER, 1 times as FAKE SENDER and 7 times as RECIPIENT.
If you want more informations about the addresses connected to the the domain you have searched write us an email at info@haveibeenemotet.com using an address from the domain you have searched (only for custom domains).

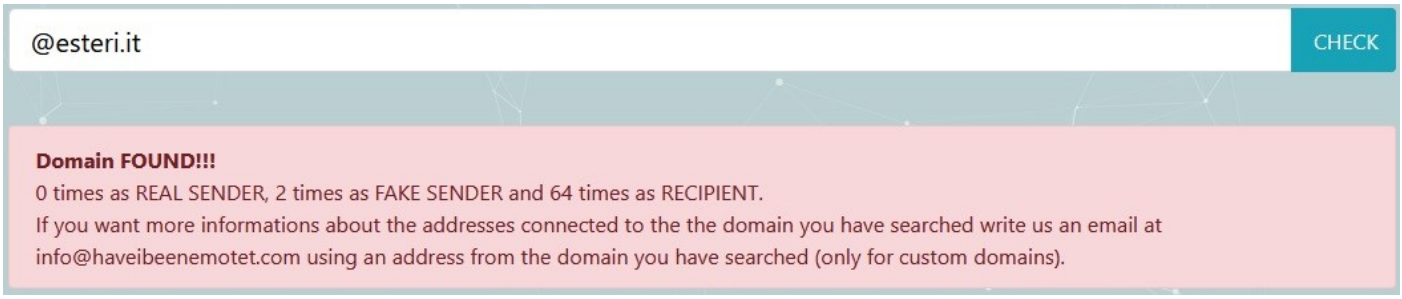
Comune di Bologna



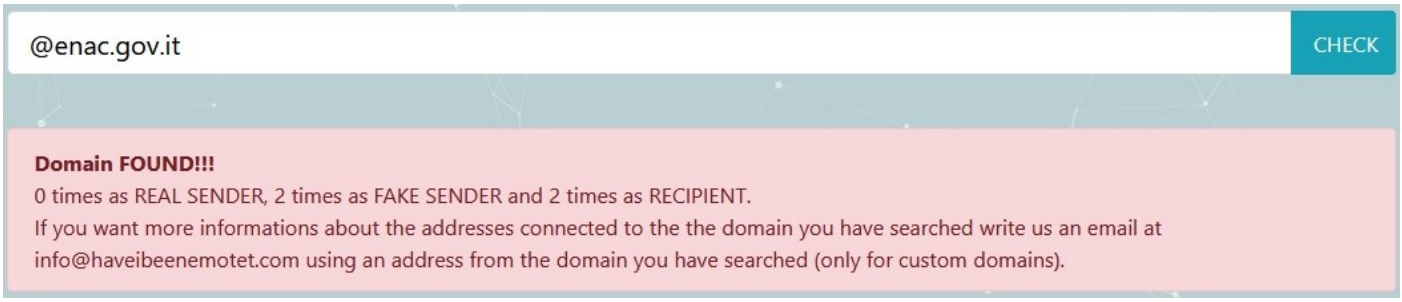
Ministero delle Infrastrutture e dei Trasporti



Ministero degli Affari Esteri e della Cooperazione Internazionale



ENAC (Ente Nazionale per l'Aviazione Civile)



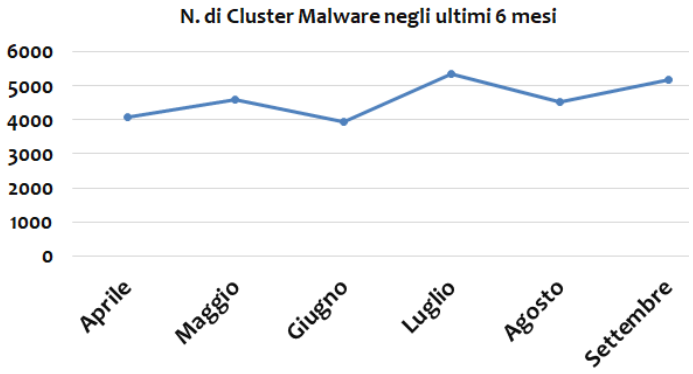
Vuoi provare dal vivo come funziona haveibeenEMOTET?

Collegati al sito https://www.haveibeenemotet.com e prova a cercare il tuo indirizzo email o il tuo dominio, oppure divertiti a scoprire com'è la situazione in Italia cercando i domini istituzionali come ad esempio @regione.lazio.it

Statistiche Malware

Settembre 2020—ITALIA

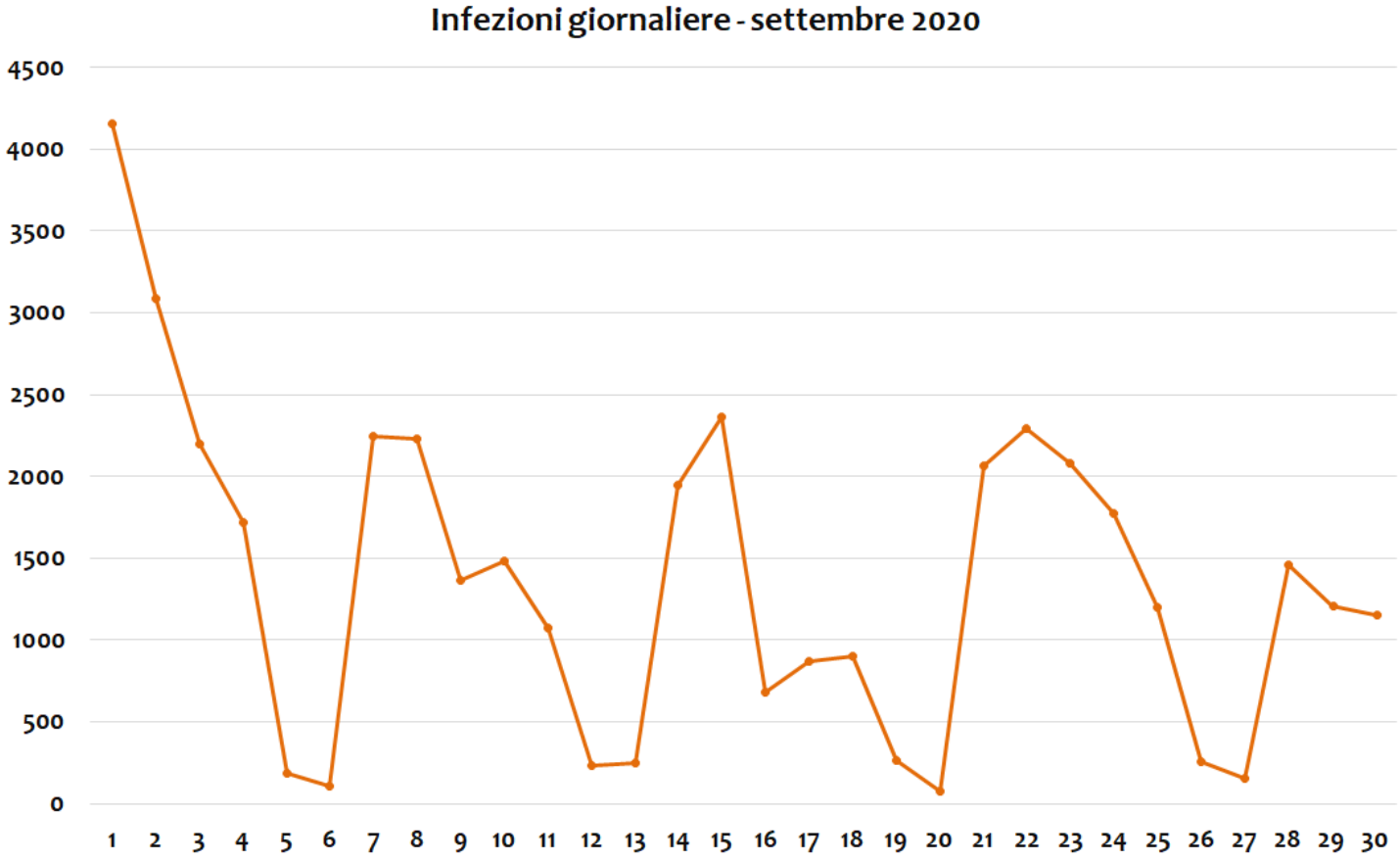
I dati della telemetria del C.R.A.M. di TG Soft sono raccolti dagli utenti che utilizzano il software anti-virus Vir.IT eXplorer. Le segnalazioni derivano da attacchi bloccati oppure malware riscontrati all'interno del parco macchine monitorato. Ogni minaccia identificata da Vir.IT viene classificata 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 settembre abbiamo avuto un incremento del numero di malware rispetto al precedente mese di agosto, dove erano stati riscontrati 4527 cluster di malware contro i 5195 del mese di settembre (+14,8%).

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 due settimane successive, abbiamo un incremento nei giorni di lunedì e martedì, per poi calare in modo progressivo nei giorni successivi. Dal 21 settembre in poi, notiamo invece un incremento delle segnalazioni, queste dovute ad un maggiore volume di spamming del malware Emotet, per poi calare leggermente solo dal 28 settembre in poi.



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

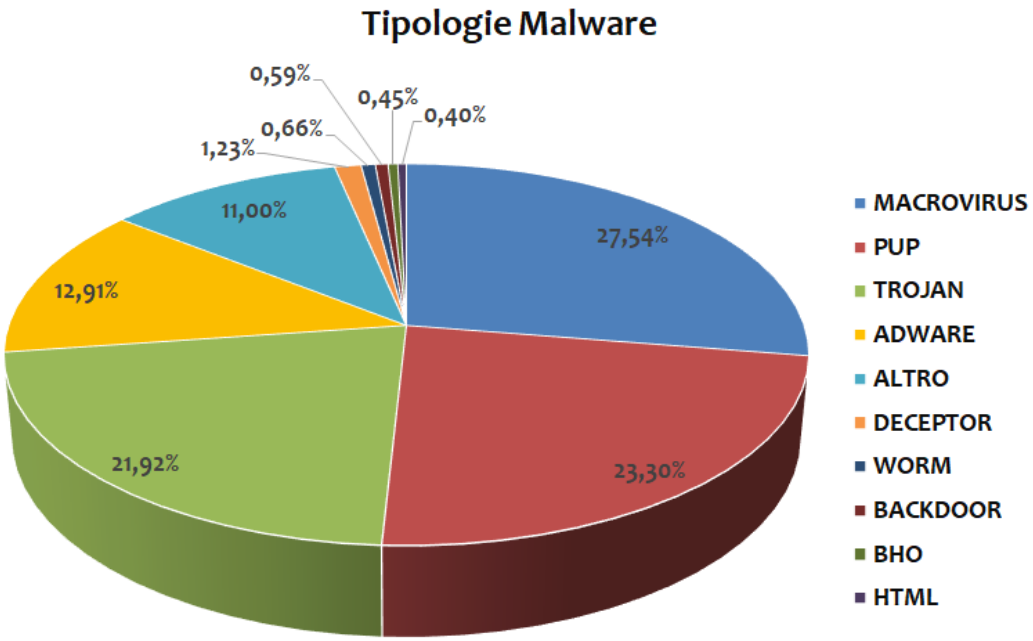
I malware si suddividono in diverse tipologie: Adware, Backdoor, Trojan, Worm, Virus, PUA/PUP, Deceptor, etc.

Nel mese di settembre la tipologia dei **MACROVIRUS** conquista la prima posizione con il 27,54% delle infezioni, relegando la famiglia dei **PUP** al secondo posto. Questa impresa dei **MACROVIRUS** deriva dall'altissimo volume di spamming di **Emotet** registrato in questo mese. Al terzo posto troviamo i **TROJAN** con il 21,92%, in calo rispetto ad agosto. Gli **ADWARE** si mantengono al quarto posto con un 12,91% anche se in calo di oltre un punto percentuale.

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

Al quinto posto troviamo il gruppo denominato **ALTRO**, che include i virus, con l'11% delle infezioni in leggero calo rispetto al mese scorso. In sesta posizione troviamo i **DECEPTOR** con l'1,23% che guadagnano una posizione rispetto ad agosto, seguono **WORM** con lo 0,66% e chiudono la classifica: **BACKDOOR; BHO** e **HTML.**

MACROVIRUS: conquistano la prima posizione, scalzando la famiglia dei PUP, grazie all'altissimo volume di spamming di Emotet registrato nel mese di settembre.



Analizziamo le statistiche di settembre dei singoli Malware. Questo mese si conferma al primo posto l'**Office.VBA_Macro_Heur** (tipologia MACRO VIRUS) , che s'impenna sfiorando il 16% delle infezioni, un incremento di ben 6 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 secondo posto troviamo il de-troneggiato **PUP.Win32.MindSpark** con la solita variante "F" con il 4,97% 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.Sality.BH** con l'1,38% delle infezioni. Il virus Sality si propaga infettando i file eseguibili, il vettore di infezione potrebbe essere legato al download di software infetto o da altri malware.

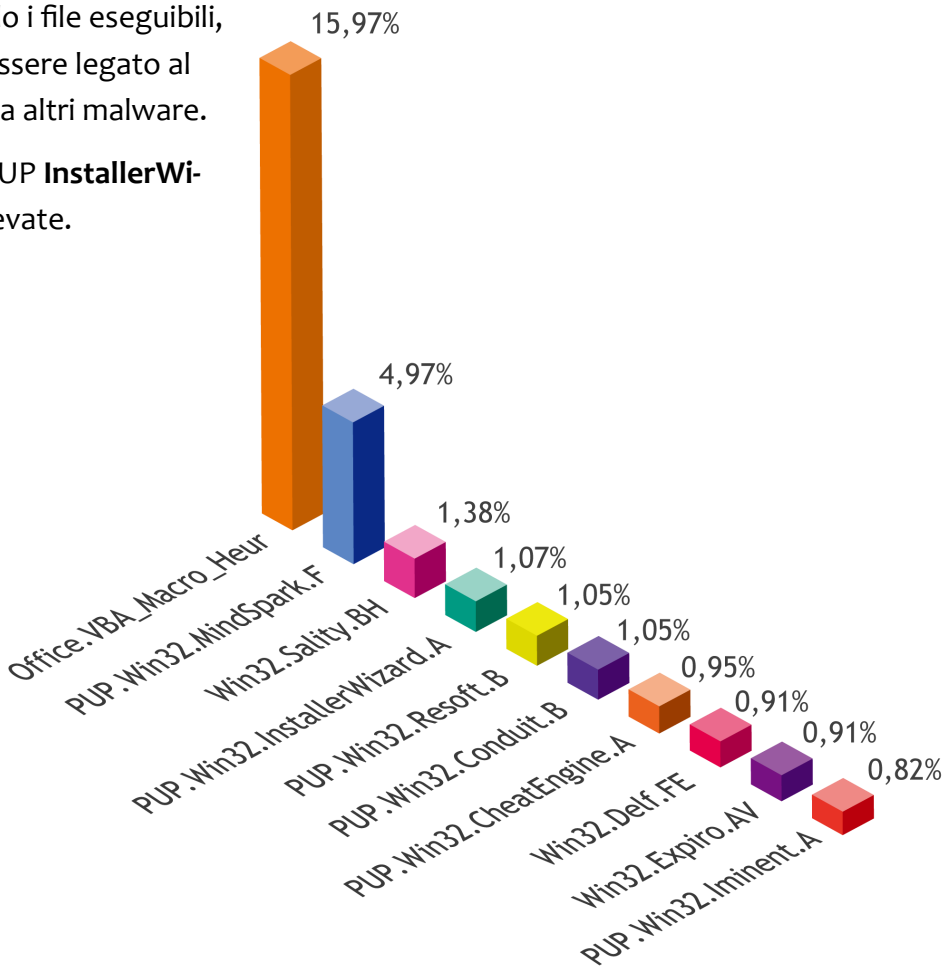
In quarta posizione troviamo il PUP **InstallerWizard** con l'1,07% delle infezioni rilevate.

I malware della Top10 rappresentano il 29,08% delle infezioni di settembre, il rimanente 70,92% è dato da altri 5185 cluster di malware.

Anche questo mese nella Top10 troviamo altre due vecchie conoscenze del mondo dei virus, sono il virus **Win32.Delf.FE** (in ottava posizione) e il **Win32.Expiro.AV** in nona posizione.

Nella Top10 troviamo ben 6 tipologie differenti di PUP, 3 tipologie virus e la tipologia dei macrovirus generici.

I malware della Top10 rappresentano il 29,08% delle infezioni del mese di settembre, il rimanente **70,92%** è dato da altri 5185 cluster di malware.

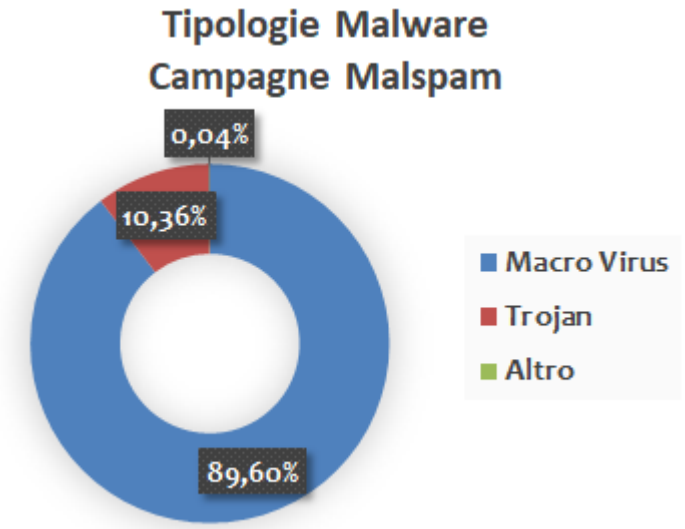


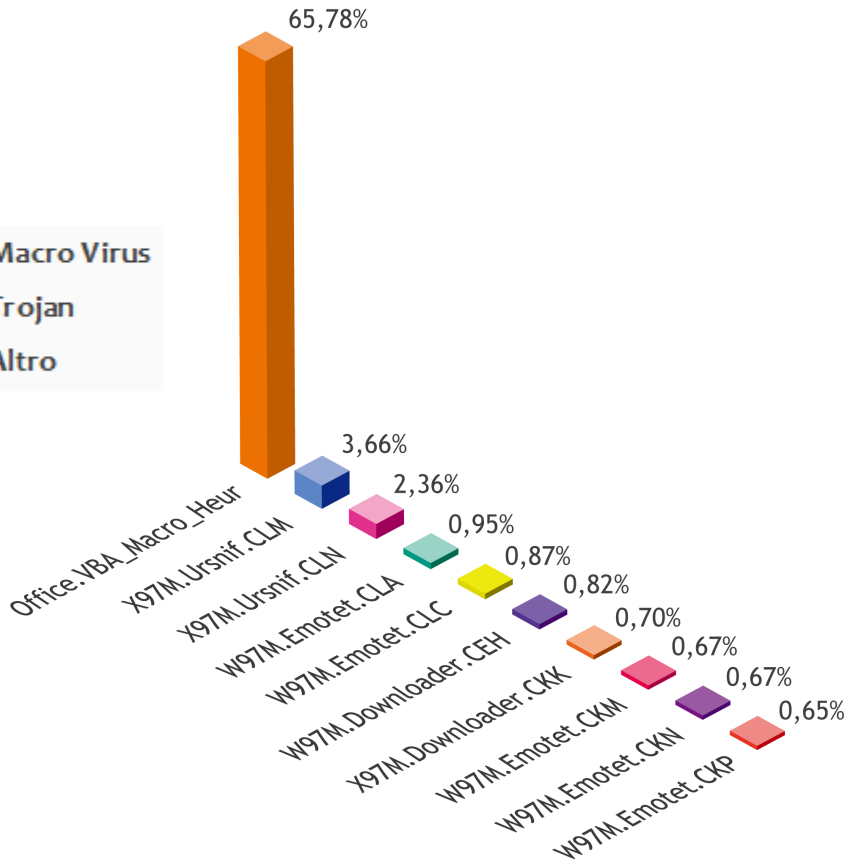
Statistiche Malware via email

Settembre 2020—ITALIA

Analizziamo ora le campagne di malware veicolate via email nel mese di settembre. 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 89,60% (+3,77%). Il dato ottenuto, segna un ulteriore incremento rispetto al mese scorso, grazie alle massive campagne di malspam di Emotet. Seguono la tipologia dei **TROJAN** che con il 10,36% (-3,66%) si confermano al secondo posto. Al terzo posto troviamo la tipologia **ALTRO** con lo 0,04% 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 65,78%. Al secondo e al terzo posto troviamo il trojan bancario chiamato **Ursnif** con le varianti **.CLM** e **.CLN**, staccate di oltre 60 punti percentuali dalla prima posizione. Nella Top10 troviamo altre cinque varianti di Emotet, rispettivamente in quarta, quinta, ottava, nona e decima posizione. Sempre appartenente alla tipologia dei MACRO VIRUS, troviamo il **W97M.Downloader.CEH** in sesta posizione, seguito da **X97M.Downloader.CKK** .

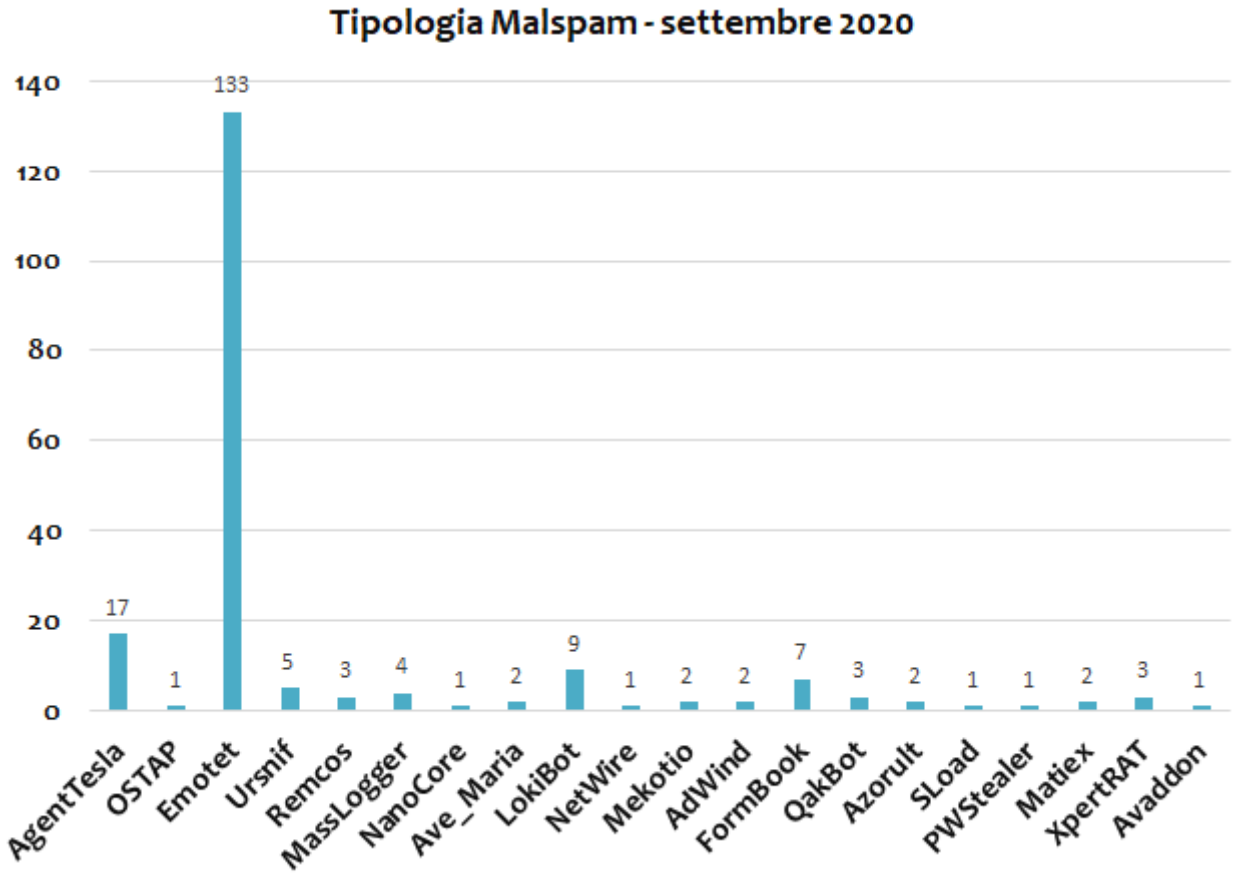
Nella Top10 delle mail, troviamo esclusivamente MACRO VIRUS, che rappresentano il 77,13% delle infezioni di settembre, il rimanente 22,87% è dato da altri 472 malware.

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

Analisi dei malware di settembre

Nel mese di settembre in Italia, attraverso le campagne di malspam che hanno "targettizzato" l'utenza italiana (email scritte in lingua italiana), sono stati veicolati 20 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 settembre.



A settembre **Emotet** regna incontrastato con 133 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.

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

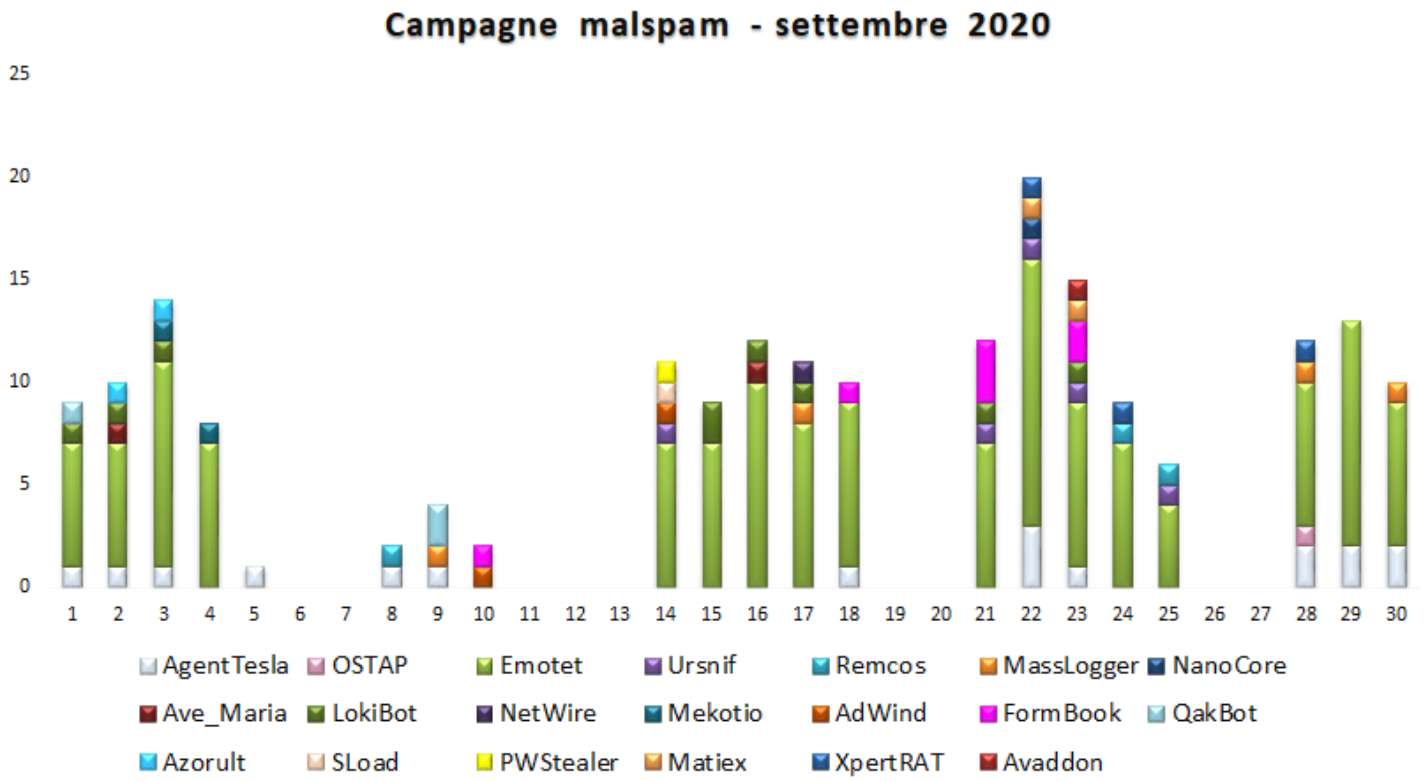
Sia **LokiBot** sia **FormBook** continuano ad essere molto utilizzati, li troviamo a settembre rispettivamente con 9 e 7 campagne. Invece il trojan banker **Ursnif** ha un leggero incremento rispetto ad agosto. ma ancora sotto alla sua media abituale. Lo scopo di questo malware è di rubare le credenziali di accesso all'home banking per svuotare il conto corrente.

A settembre nuove famiglie di malware si sono affacciate nel panorama italiano, tra questi possiamo citare **Mekotio**, **Matiex** e **XpertRAT**, che hanno la capacità di carpire le credenziali e spiare il computer infetto.

Sono continuate le campagne di **QakBot** e **OSTAP**, e sono ritornati **SLoad** e il ransomware **Avaddon**. A settembre non abbiamo riscontrato gli attacchi di **Hagga,** che si era fatto notare nei mesi scorsi.

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

Nel mese di settembre Emotet ha "spammato" quasi tutti giorni, tranne la settimana dal 7 al 13. Il picco delle campagne nel mese è avvenuto martedì 22 settembre , dove sono state diffuse 20 campagne di malspam, che hanno veicolato 6 differenti famiglie di malware.



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

Week 35 ==> dal 29 agosto al 4 settembre

Week 36 ==> dal 5 all'11 settembre

Week 37 ==> dal 12 al 18 settembre

Week 38 ==> dal 19 al 25 settembre

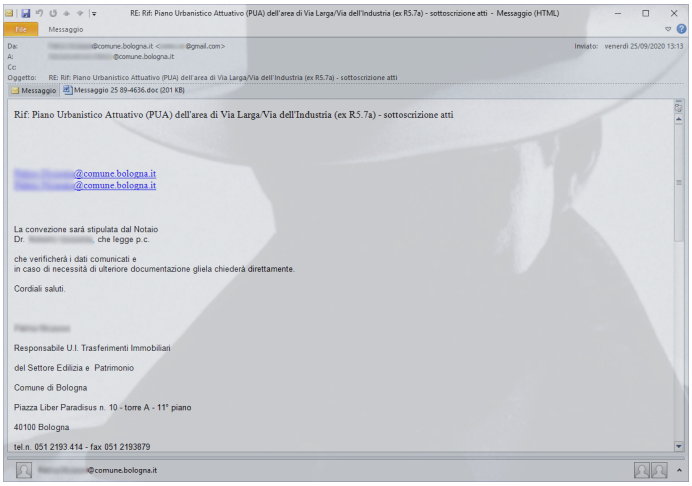
Week 39 ==> dal 26 settembre al 2 ottobre

Emotet

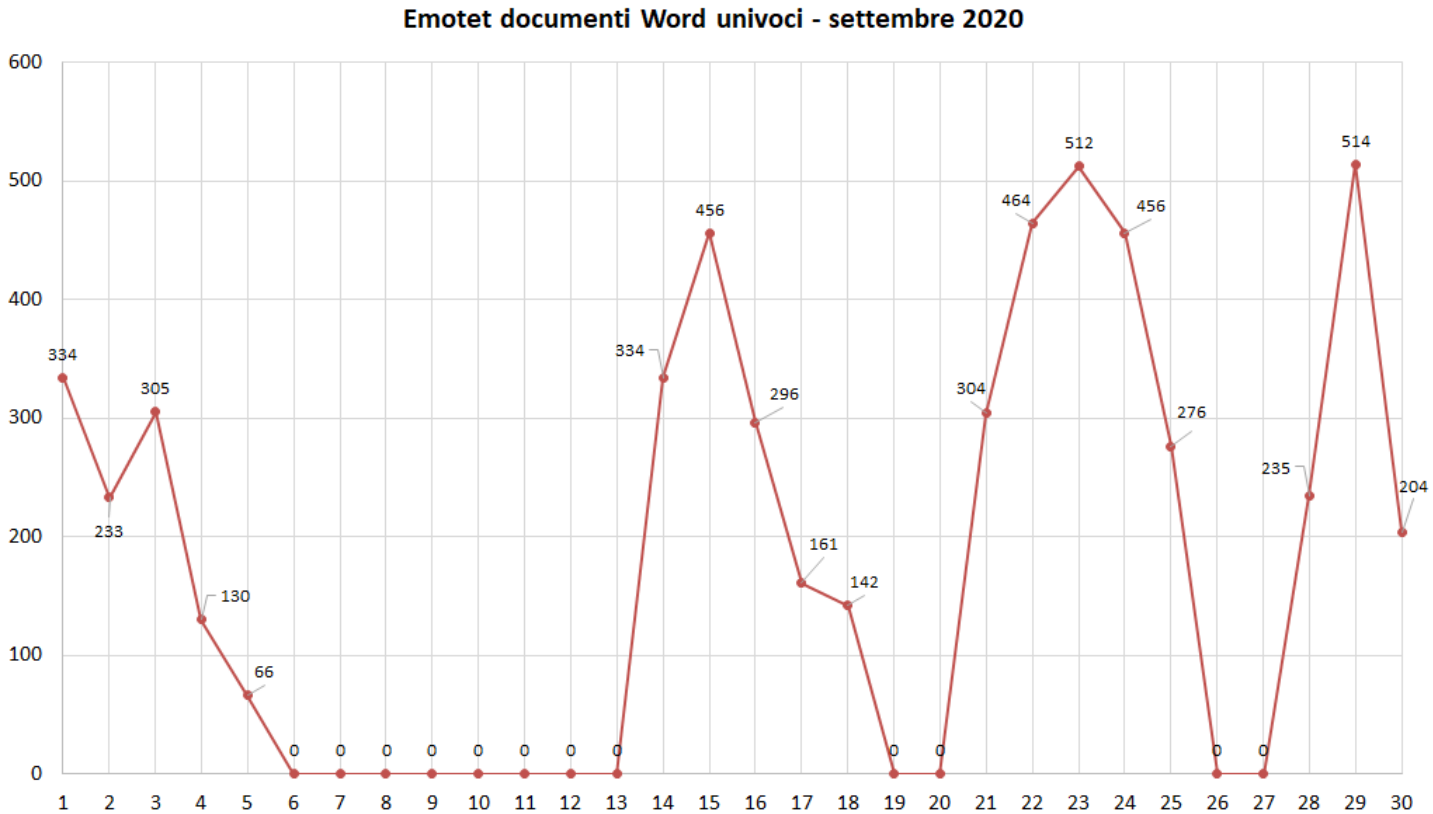
Analisi delle campagne di settembre

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

Nell'immagine a destra vediamo un esempio di email del 25 settembre del Comune di Bologna con allegato un documento di Word infetto da Emotet.



Nella prima settimana di settembre, Emotet ha spammato un gran volume di campagne. Nella settimana successiva abbiamo registrato una pausa nelle campagne di malspam. Dal 14 settembre Emotet ha ripreso a spammare massivamente in Italia fino alla fine del mese. Nella figura sottostante possiamo vedere l'andamento giornaliero dei documenti di Word univoci infetti da Emotet distribuiti via email nel mese di settembre. Come possiamo vedere dal grafico, il numero di documenti distinti allegati alle campagne di malspam di Emotet, registra il suo picco massimo (con 514 hash univoci) martedì 29 settembre. A partire dalla metà del mese è stato registrato un aumento del volume di spam, molto probabilmente dovuto all'incremento del numero delle vittime. 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.



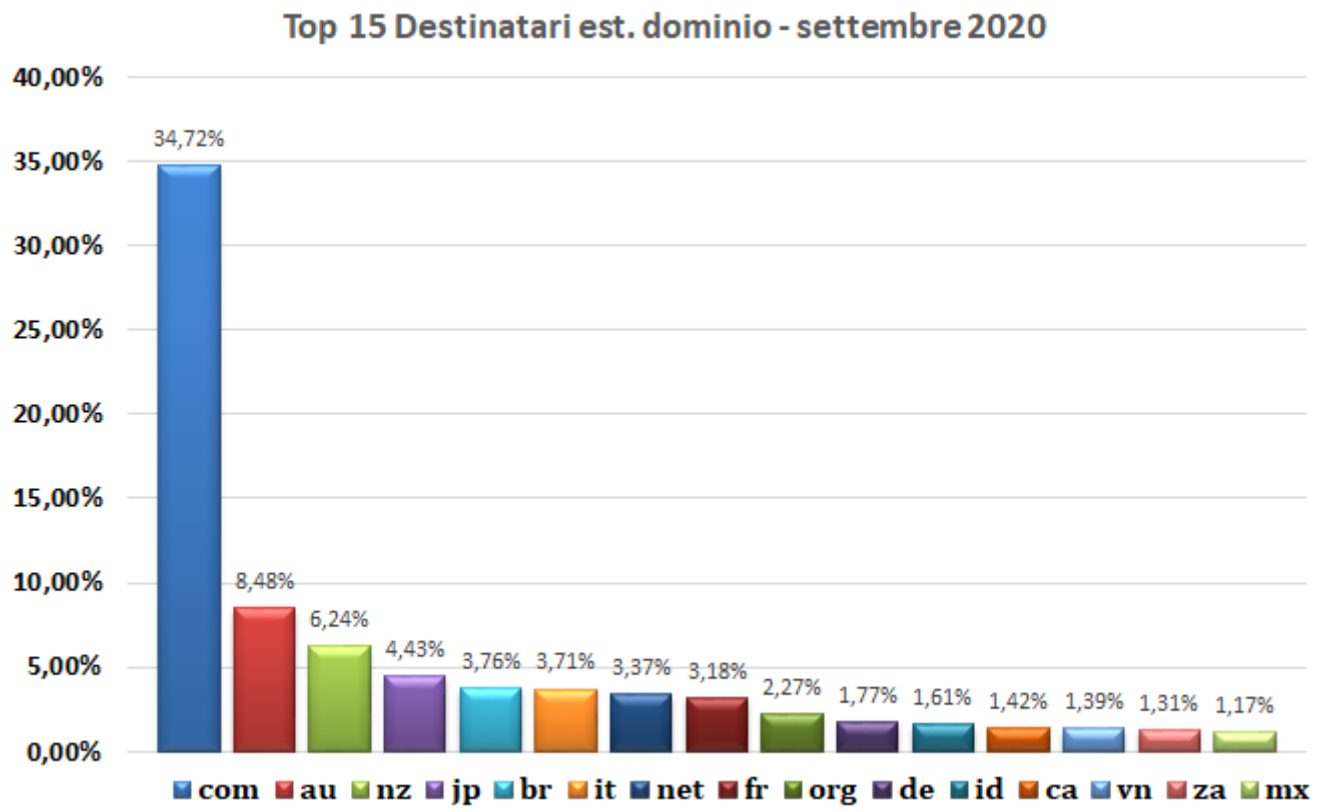
Questa tecnica, nota come "*thread hijacking*" di rispondere alle email rubate, falsificando il mittente originale, inganna il destinatario del messaggio che, in buona fede, procedendo ad aprirlo, si infetterà. Questa tecnica è stata utilizzata in passato dal malware **Ursnif**.

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 700.000 email monitorate dal C.R.A.M. nel mese di settembre.

Al primo posto troviamo con oltre il 34% 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'8.48% gli indirizzi email "**.au**" dell'**Australia**. La **Nuova Zelanda** si posiziona al terzo posto con il 6,24% . Il **Giappone** (jp) si posiziona al quarto posto, davanti al **Brasile** (br), **Italia** (it), **Francia** (fr) e **Germania** (de).

L'**Italia** fa un notevole balzo dalla 31-esima posizione di agosto alla 6ª di settembre con il 3,71% delle email inviate verso indirizzi "**.it**".

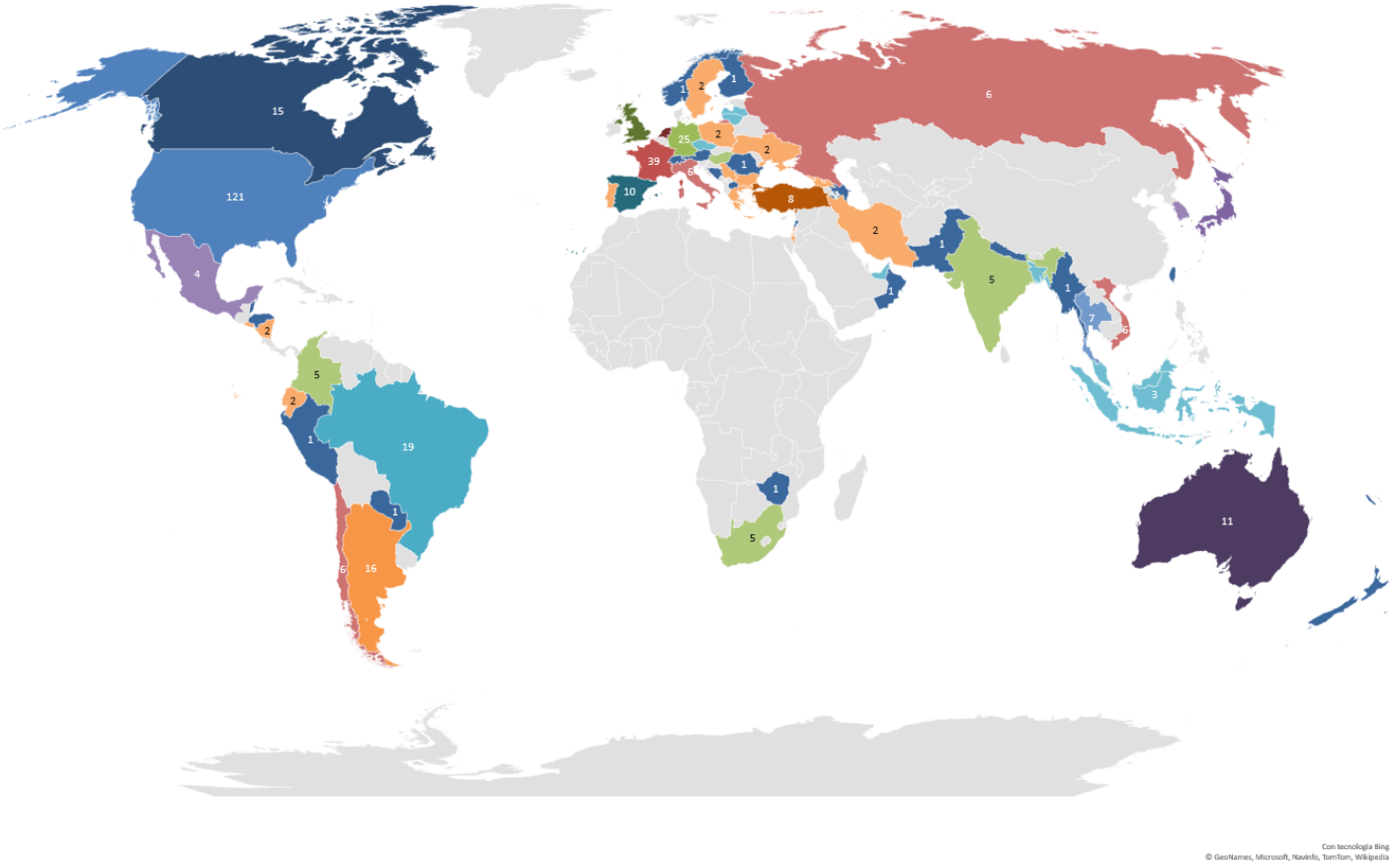


Le informazioni rubate dai computer delle vittime vengono inviate ad una serie di server di comando e controllo dell'Emotet. Questi computer che hanno la funzione di server C&C sono distribuiti in tutto il mondo.

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

A settembre Emotet si è collegato a più di **456 server C&C**. La maggior parte di questi si trovano negli **Stati Uniti d'America (121 server)**, come possiamo vedere nella tabella a fianco. Al secondo e terzo posto troviamo rispettivamente Francia e Germania. L'**Italia** si posiziona al sedicesimo posto con **6 server** di comando e controllo.

Stato	Num. Server C2
Stati Uniti	121
Francia	39
Germania	25
Giappone	23
Brasile	19
Argentina	16
Canada	15
Olanda	13
Gran Bretagna	12
Australia	11
Singapore	11
Spagna	10
Turchia	8
Tailandia	7
Chile	6
Italia	**6**
Altri Paesi	114



In Italia vi sono 6 server di comando e controllo, come possiamo vedere dalla seguente tabella:

IP	Città	Provider
185.178.10.77	Apice	Lo Conte WiFi s.r.l.
188.219.31.12	Torino	Vodafone Italia S.p.A.
93.147.212.206	Agrigento	Vodafone Italia S.p.A.
2.36.95.106	Bussero	Vodafone Italia S.p.A.
130.0.132.242	Milano	Vodafone Italia S.p.A.
2.47.112.152	Napoli	Vodafone Italia S.p.A.

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.**

Ursnif

Analisi delle campagne di settembre

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

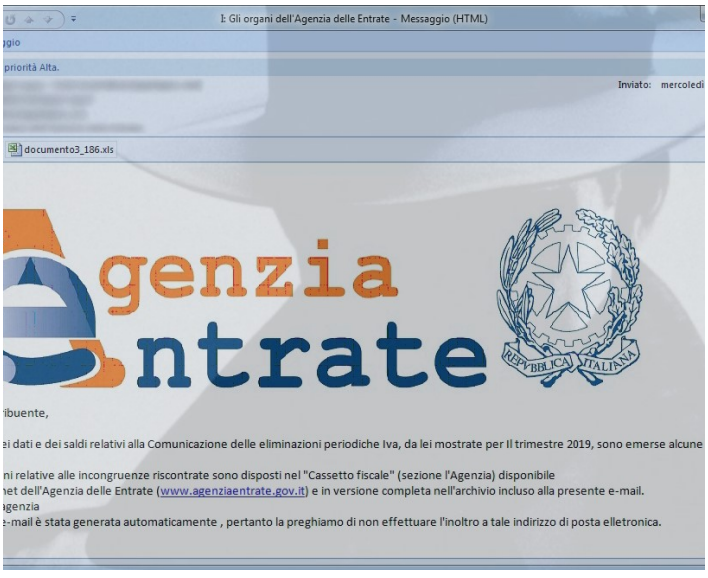
Come abbiamo visto, questo malware è uno dei più diffusi via email in Italia, ma a settembre è stato veicolato solamente attraverso 5 campagne di malspam.

Come si può vedere dalla figura a fianco, l'andamento delle campagne ne ha risentito nelle prime settimane di settembre, solamente a partire dal 21 settembre si è registrato un incremento di malspam di Ursnif.

A metà del mese fa capolino la prima campagna a tema "INPS" e dal giorno 21 in poi sono susseguite altre campagne a tema "Agenzia delle Entrate", "Bonifico BRT S.p.a" e "Organizzazione Mondiale della Sanità".

Ursnif—Campagne Malspam

14/09/2020	INPS
21/09/2020	Agenzia delle Entrate
22/09/2020	Bonifico BRT S.p.a.
23/09/2020	Agenzia delle Entrate
25/09/2020	Org. Mondiale della Sanità

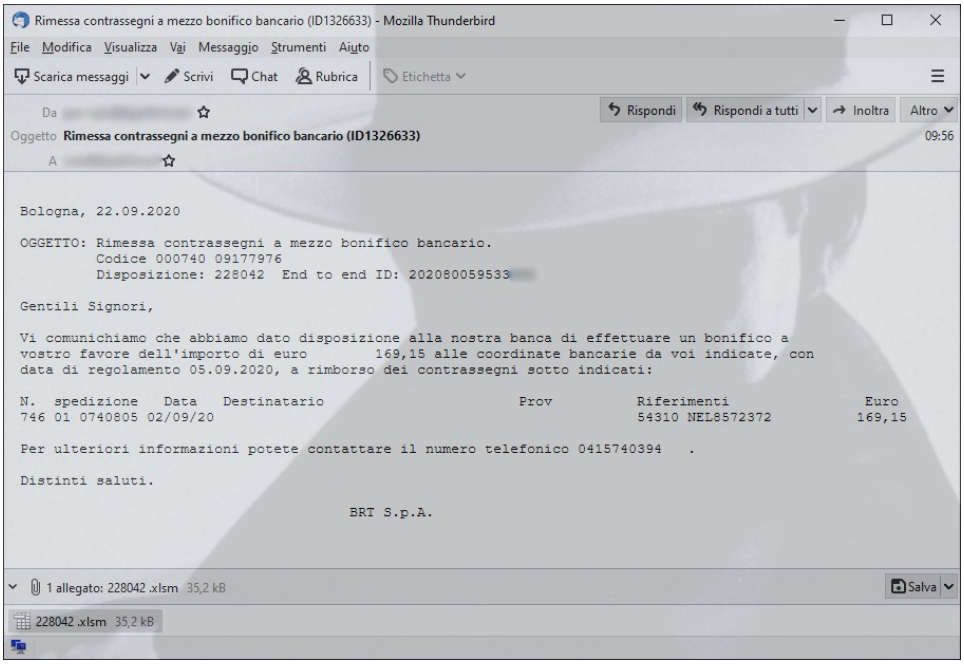


A settembre i cyber-criminali sfruttano il nuovo tema dell'Organizzazione Mondiale della Sanità per veicolare Ursnif

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 settembre per attaccare l'utenza italiana.

A settembre i cyber-criminali sfruttano il nuovo tema dell'Organizzazione Mondiale della Sanità per veicolare Ursnif oltre ai vecchi temi dell'Agenzia delle Entrate e dell'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 segnalato. 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 mese di settembre, come era successo ad agosto, non vi sono stati aggiornamenti nel malware Ursnif, la build utilizzata nelle varie campagne dai due gruppi è sempre stata la stessa, la 154.

Ransomware

Settembre 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:

- **LockBit**
- **Makop**
- **Crysis**
- **Avaddon**
- **Phobos**

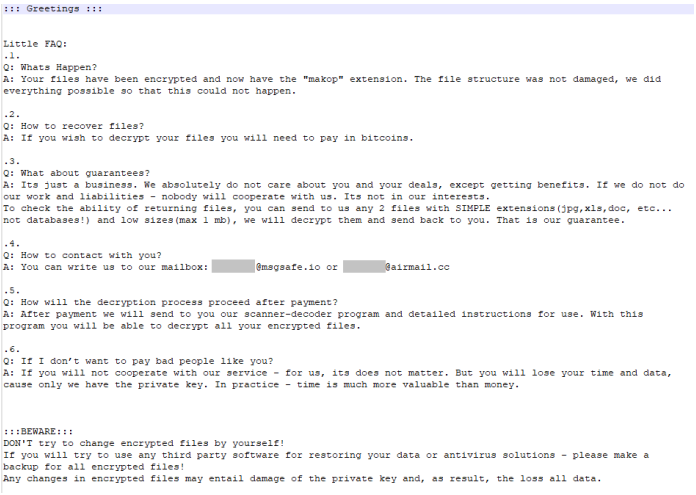
I ransomware identificati a settembre derivano da attacchi attraverso il desktop remoto (RDP) mirati verso aziende italiane, campagne di malspam e navigazione su siti compromessi.

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.

Makop non è un ransomware nuovo, ne abbiamo già parlato nei mesi scorsi. L'attacco in questione è avvenuto via RDP nella serata dell'8 settembre, con la seguente cronologia di operazioni:

1. **2020-09-08 20:09:26** primo tentativo di esecuzione del ransomware;
2. **2020-09-08 20:10:34** tentativo di disinstallazione dell'anti-virus;
3. **2020-09-08 20:20:12** secondo tentativo di esecuzione del ransomware;
4. **2020-09-08 20:26:42** terzo tentativo di esecuzione del ransomware
5. **2020-09-08 20:52:15** quarto tentativo di esecuzione del ransomware

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



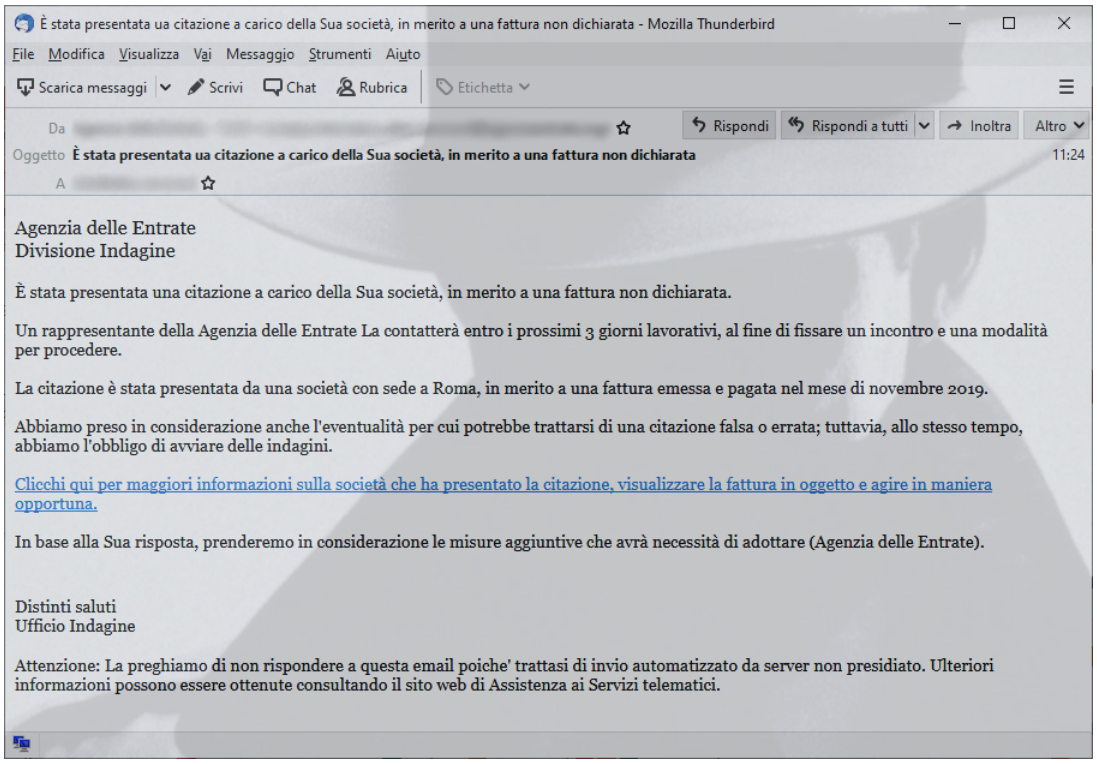
```
::: Greetings :::

Little FAQ:
.1.
Q: Whats Happen?
A: Your files have been encrypted and now have the "makop" extension. The file structure was not damaged, we did
everything possible so that this could not happen.

.2.
Q: How to recover files?
A: If you wish to decrypt your files you will need to pay in bitcoins.

.3.
Q: What about guarantees?
A: Its just a business. We absolutely do not care about you and your deals, except getting benefits. If we do not do
our work and liabilities - nobody will cooperate with us. Its not in our interests.
To check the ability of returning files, you can send to us any 2 files with SIMPLE extensions(jpg,xls,doc, etc...
not databases!) and low sizes(max 1 mb), we will decrypt them and send back to you. That is our guarantee.

.4.
Q: How to contact with you?
A: You can write us to our mailbox: [redacted]@msgsafe.io or [redacted]@airmail.cc

.5.
Q: How will the decryption process proceed after payment?
A: After payment we will send to you our scanner-decoder program and detailed instructions for use. With this
program you will be able to decrypt all your encrypted files.

.6.
Q: If I don't want to pay bad people like you?
A: If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data,
cause only we have the private key. In practice - time is much more valuable than money.


:::BEWARE:::
DON'T try to change encrypted files by yourself!
If you will try to use any third party software for restoring your data or antivirus solutions - please make a
backup for all encrypted files!
Any changes in encrypted files may entail damage of the private key and, as result, the loss all data.
```

L'accesso remoto (RDP) è avvenuto da un computer di una società italiana con base a Vicenza, che era abilitata ad accedere al computer colpito, perché fornitrice di servizi gestionali. L'attacco ha coinvolto in primis la società vicentina, da cui i cyber-criminali hanno individuato un computer abilitato a collegarsi via RDP ad altre società esterne. I cyber-criminali hanno quindi sfruttato il computer adibito alla manutenzione remota per accedere a computer di società esterne per sferrare l'attacco ransomware.

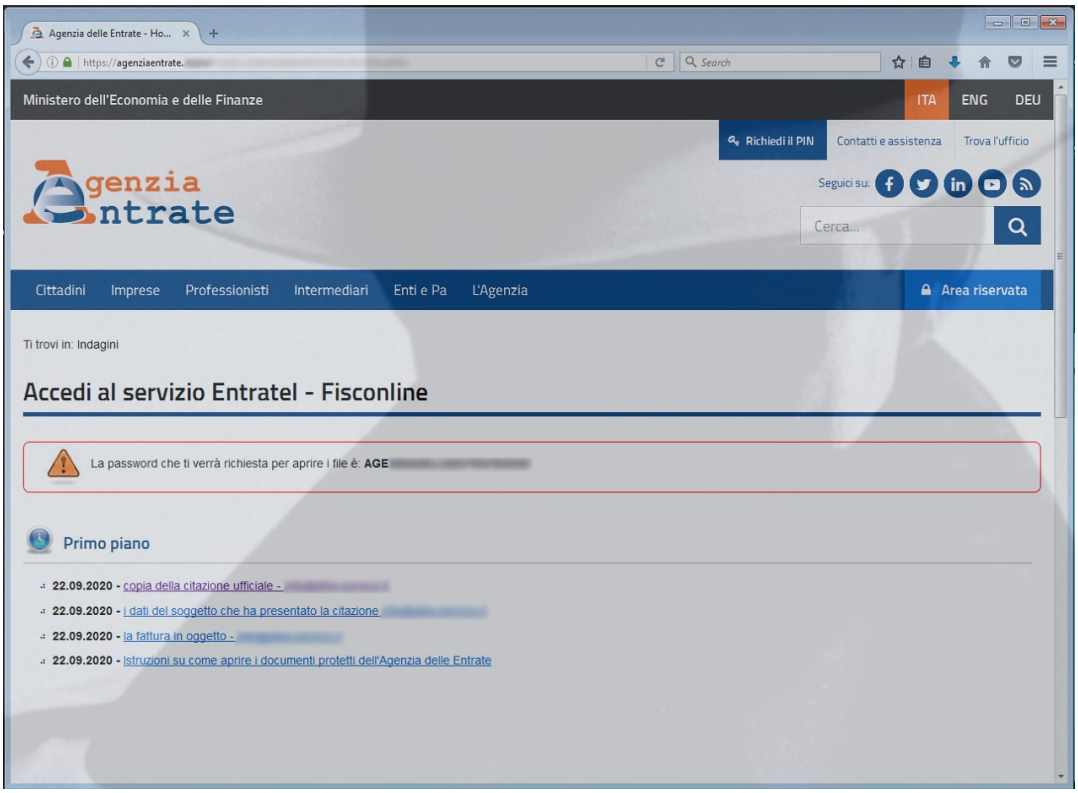
Nel mese di settembre è stata individuata una campagna di malspam atta a veicolare il ransomware della famiglia **Avaddon**.

La campagna di malspam con oggetto "*È stata presentata ua citazione a carico della Sua società, in merito a una fattura non dichiarata*", si spacciava come provenire dall'Agenzia delle Entrate e conteneva un link malevolo che re-indirizzava la vittima verso un finto portale dell'Agenzia delle Entrate.

Nell'immagine sottostante possiamo vedere la mail incriminata con il link che veicola **Avaddon.**



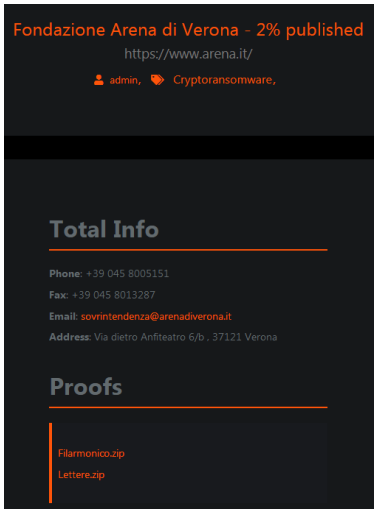
Nell'immagine sottostante possiamo vedere il finto portale dell'Agenzia delle Entrate da cui veniva scaricato il ransomware **Avaddon.**

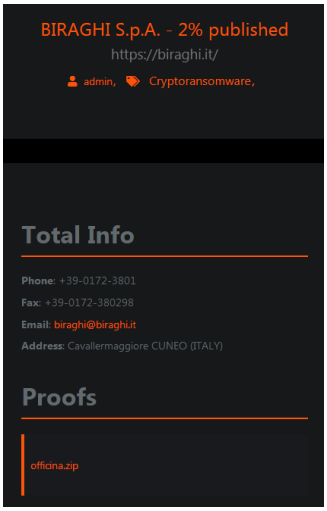


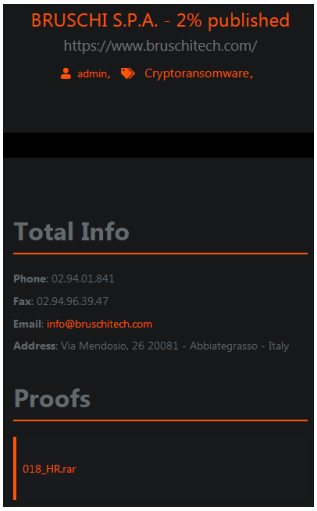
A settembre il gruppo cyber–criminale del **Maze** ha attaccato altre quattro società italiane:

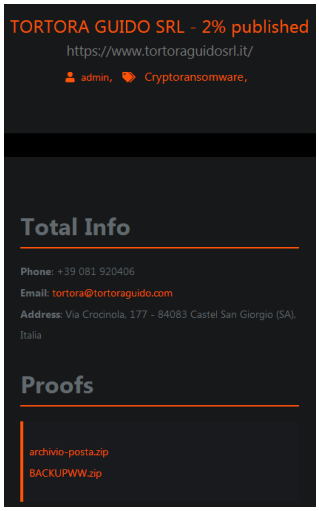
- Fondazione Arena di Verona (Verona)
- Biraghi S.p.a. (Cavallermaggiore - Cuneo)
- Bruschi S.p.a. (Abbiategrasso - Milano)
- Tortora Guido S.r.l. (Castel San Giorgio - Salerno)

Per tutte le vittime sono stati pubblicati una parte delle informazioni riservate esfiltrate durante l'attacco.

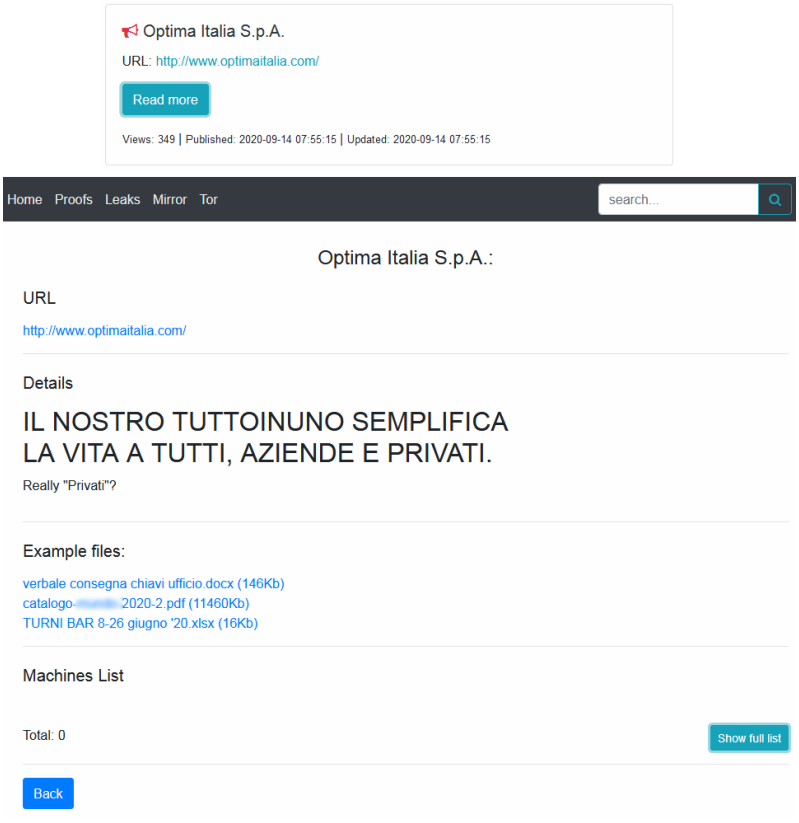








Per quanto riguarda il ransomware **DoppelPaymer**, i cyber-criminali affermano a settembre di aver attaccato la società **Optima Italia S.p.a.** con esfiltrazione di documenti riservati, come mostrato nelle immagine a fianco.



A settembre non sono finiti qui gli attacchi ransomware in Italia. Diverse testate giornalistiche e media hanno dato notizie di attacchi informatici verso **Luxottica S.p.A.** e l'**Università degli studi di Roma "Tor Vergata"**, che ha portato per la prima al blocco della produzione per l'intera giornata del 21 settembre, mentre per la seconda sono stati compromessi più di 100 computer nella notte di venerdì 4 settembre.

Nell'immagine sottostante possiamo vedere uno dei domini di Luxottica non disponibili durante l'attacco informatico.

Prevalenza

Settembre 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.

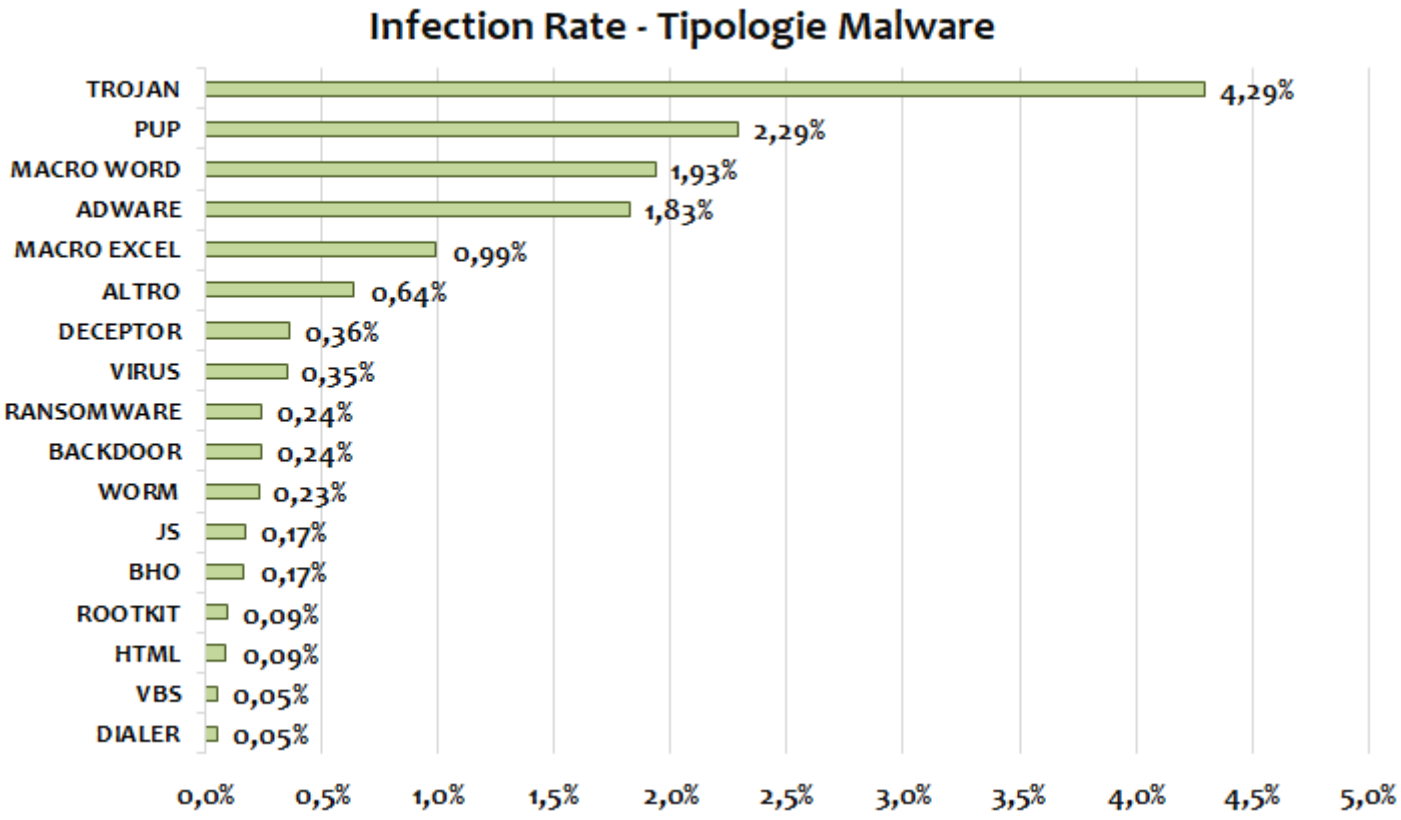
Vediamo ora i dati relativi alla prevalenza dei malware registrati dal C.R.A.M. di TG Soft nel mese di settembre. Per prevalenza si intende l'incidenza che i malware hanno in un determinato periodo. Il valore calcolato si chiama "rate di infezione".

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 del 2,29%. Terzo gradino del podio per la categoria dei **MACRO WORD** con l'1,93%.

Dalla 4ª alla 6ª posizione troviamo gli **Adware** , seguiti dalle **macro di Excel** e dal gruppo generico denominato **Altro** (che include le macro di Office generiche). Si attestano in 9ª posizione i **Ransomware** con lo 0,24%. 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.).

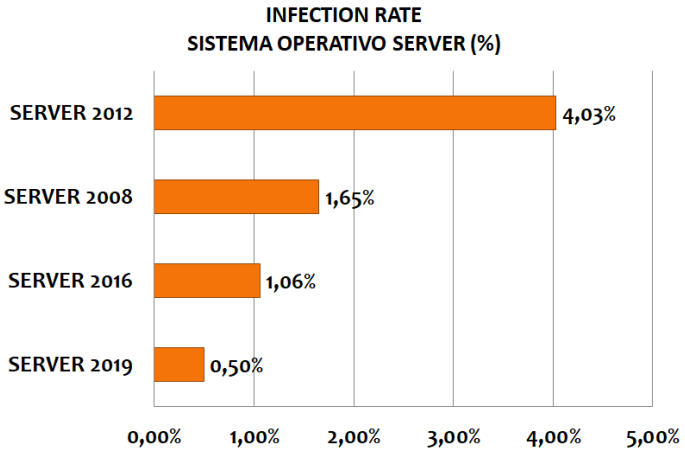


Andiamo ora ad analizzare la prevalenza delle infezioni del mese di settembre in base ai sistemi operativi suddivisi tra sistemi Server e Client.

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.

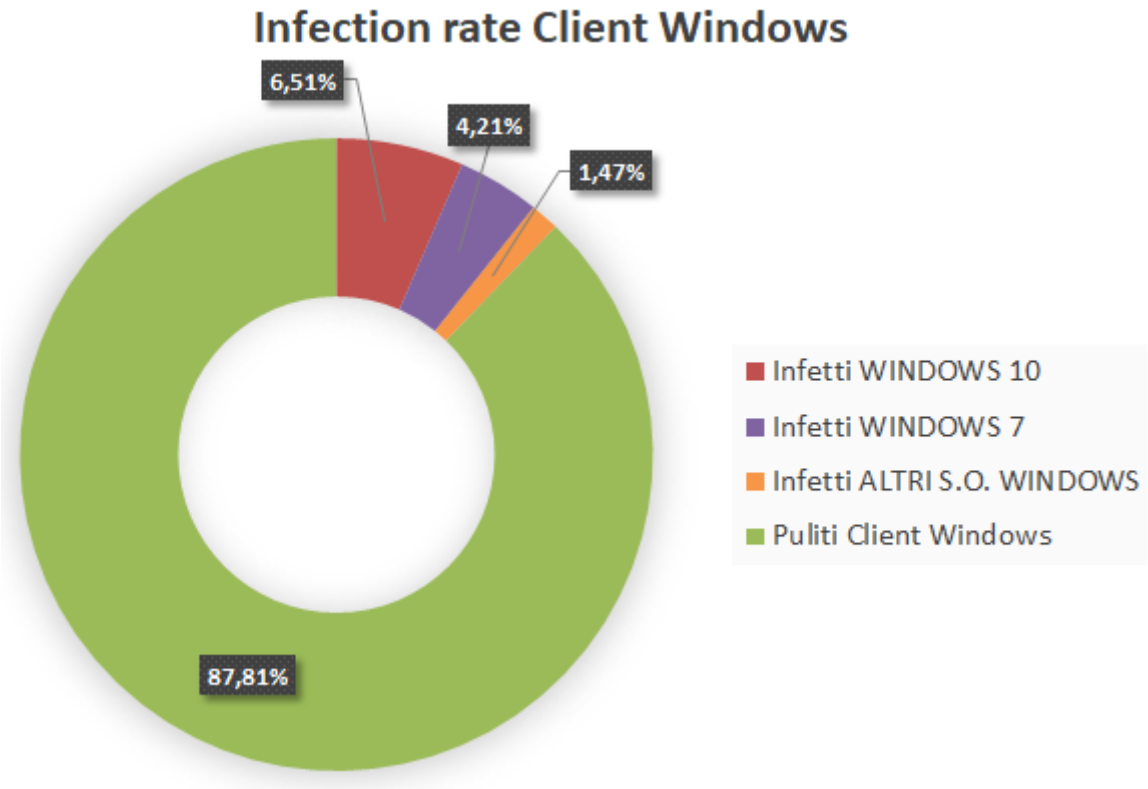
Dai dati relativi ai server, si potrebbe evincere che la probabilità dell'infezione/attacco di un Server 2019 rispetto ad un Server 2012 (più datato…) è di un ordine di grandezza inferiore 0,50% contro 4,03%.

Nelle statistiche relative alla prevalenza delle infezioni dei computer client nel mese di settembre abbiamo riscontrato che il **12,19%** dei terminali è stato infettato o ha subito un attacco. Questo dato indica che **12 computer su 100** è stato colpito da malware nel mese di settembre.



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

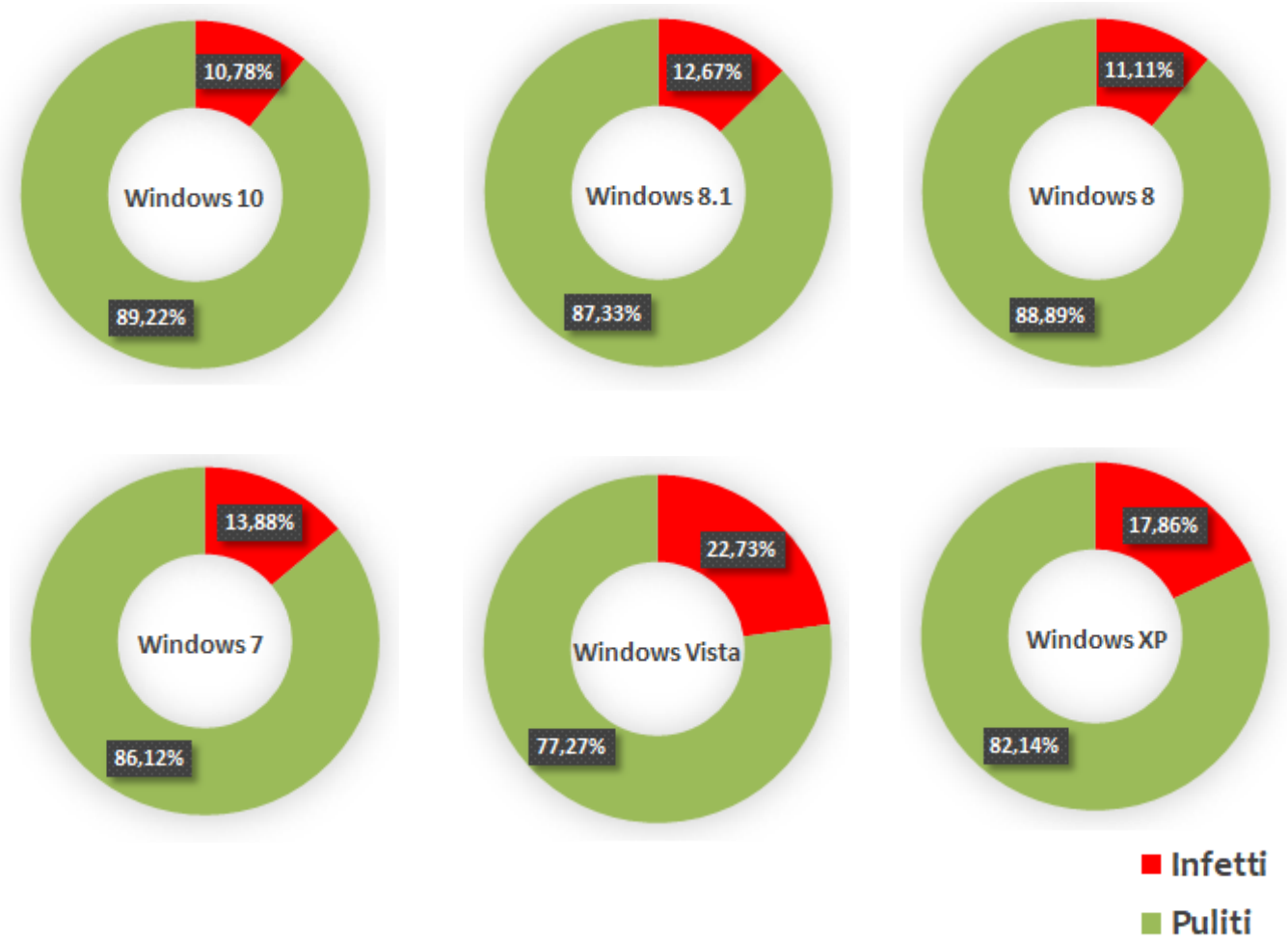
- 60,37% client con Windows 10
- 30,31% client con Windows 7
- 9,32% client con altri s.o. Windows



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 ?

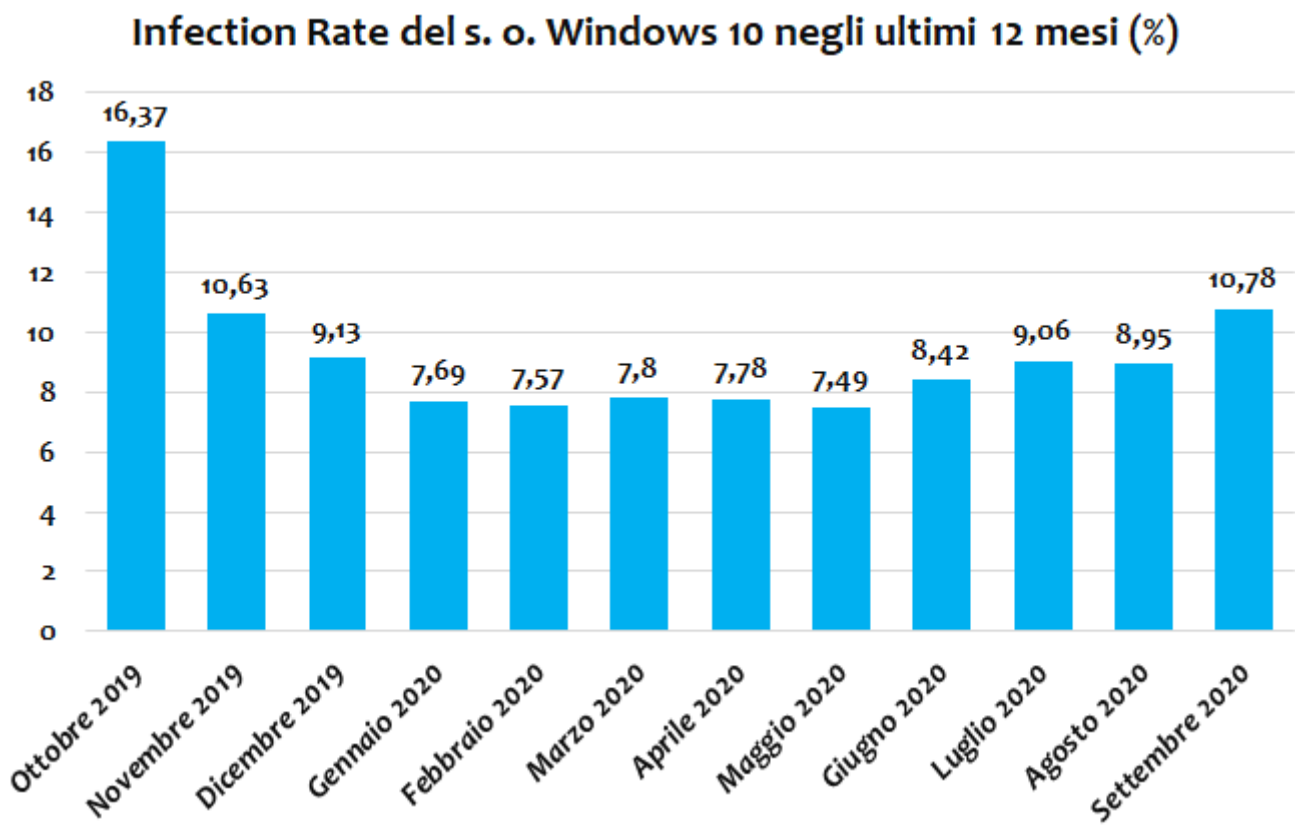
Per rispondere a questa domanda dobbiamo calcolare la prevalenza d'infezione sul medesimo sistema operativo. Prendendo ad esempio Windows 10, si può notare che il rate di infezione tra tutte le macchine ove è installato Windows 10 che ha subito un attacco informatico è del 10,78% . Con questo calcolo 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 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 settembre registriamo un incremento delle infezioni rispetto al mese di agosto. Il mese di settembre 2020 ha visto l'incremento di un punto percentuale rispetto al mese dell'anno scorso, molto probabilmente dovuto all'alto volume di malspam generato da Emotet in questo mese.



TG Soft
Cyber Security Specialist
www.tgsoft.it