Cyber-Threat Report

Febbraio 2021

TG Soft
Cyber Security Specialist
www.tgsoft.it

Febbraio 2021

TG Soft
Cyber-Threat Report

Notizie di rilievo:

sLoad ed il bonifico dirottato

Panorama delle minacce in Italia a febbraio

Sommario:

Nel mese di febbraio dopo l'abbattimento della BotNet di Emotet i malware che sono stati maggiormente veicolati e che rappresentano minacce concrete per qualsiasi utente sono, in particolare, il trojan bancario UrSnif e il Password Stealer sLoad.
Su quest'ultimo illustriamo un caso realmente andato a segno sul quale il nostro Centro Ricerche AntiMalware è stato chiamato ad effettuare un'analisi di IR (Incident-Response).
Per quanto riguarda i Ransomware la maggior parte di questi è stata veicolata attraverso attacchi via RDP maldestramente configurati dove i CyberCriminali una volta guadagnato l'accesso all'infrastruttura hanno potuto agire indisturbati "Human-operated ransomware attacks".
Nel mese di febbraio ha visto in azione, oltre ai già citati UrSnif e sLoad, le principali campagne hanno visto come protagonisti: FormBook; AgentTesla; LokiBot e QakBot.
Di interesse per la generalità, in particolare, ***sLoad ed il bonifico dirottato...***

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

TG Soft Cyber Security Specialist
www.tgsoft.it

TG Soft S.r.l.

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

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

TG Soft
Cyber Security Specialist
www.tgsoft.it

Proteggiamo il tuo business dai cyber-criminali

[www.tgsoft.it]

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

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

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

Seguici 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

sLoad ed il bonifico dirottato

Ogni giorno i nostri computer sono sotto attacco informatico, attraverso messaggi di posta elettronica contenenti malware o tentativi di accesso alla nostra rete aziendale o privata. Spesso si legge nei giornali o attraverso i media di notizie di cyber-attacchi dove viene richiesto di pagare un riscatto per recuperare i propri documenti o di aziende il cui conto corrente in banca è stato svuotato.

In questo articolo riteniamo utile ed opportuno illustrare un attacco reale da parte di organizzazioni Cyber-Criminali che sono riuscite a mettere a segno il dirottamento un bonifico verso il conto corrente del malfattore.

"Come ti dirotto il bonifico" potrebbe essere la sceneggiatura di un film di Sergio Leone, dove i tre principali personaggi sono il Buono, il Brutto e il Cattivo, invece è una storia vera dove gli attori sono un truffato, una vittima inconsapevole ed un cyber-criminale.

Nel mese di febbraio, tra le numerose richieste di analisi di #IR (IncidentResponse) che il Centro Ricerche Anti Malware [C.R.A.M.] di TG Soft è stato chiamato ad analizzare, si ritiene utile ed opportuno, quale attività didattico-divulgativa illustrare un incidente di cyber security, oramai abbastanza tipico, che ha avuto come risultato un danno economico reale quale il dirottamento di un bonifico.

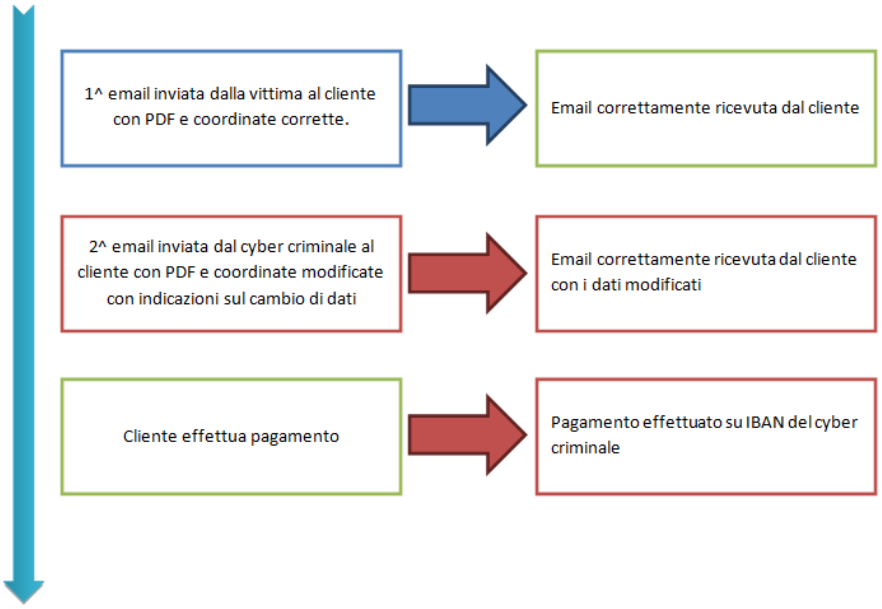
In sintesi in un comunissimo rapporto Cliente-Fornitore si intrometteva un CyberCriminale che prima riusciva ad ottenere l'accesso alla casella di posta elettronica del fornitore così da poterne leggere le mail e poi procedeva a dirottarne una parte per perpetrare la truffa ai danni sia del fornitore come anche del cliente.

Fase di ANALISI PRELIMINARE

Come prima attività il C.R.A.M. di TG Soft dopo consulto con il fornitore, che per proteggerne l'identità chiameremo con un nome di fantasia "Anna" ha proceduto a riassumere i fatti accaduti:

1) Il fornitore "Anna" spiega che al completamento di materiale termo-idraulico provvedeva ad inviare alla cliente la fattura via e-mail trattandosi di cliente privato che non aveva la possibilità di ricevere nè fattura elettronica nè PEC e quindi veniva inoltrata la cosiddetta fattura di cortesia a mezzo e-mail ordinaria;
2) la fattura veniva trasmessa come allegato in formato .PDF e riportava, naturalmente, le coordinate bancarie della ditta fornitrice dove effettuare il pagamento (IBAN) per i prodotti-servizi forniti.
3) Passati i termini concordati per il pagamento il fornitore "Anna" contattava il suo cliente per avere lumi sul bonifico a saldo della fornitura e, con una certa sorpresa, Anna veniva a conoscenza che il cliente aveva già effettuato il pagamento, riferendosi alle coordinate presenti nel PDF che presumeva aver ricevuto tramite email dal fornitore, ma che invece erano state modificate ad arte dal Cyber-Criminale;
4) Confrontando infatti le e-mail ricevute dal cliente con quelle originali che il fornitore "Anna" aveva effettivamente redatto ed inviato, si scopriva che a seguito del primo .PDF con le coordinate bancarie corrette, il cliente aveva ricevuto una seconda e-mail modificata ad arte dal Cyber-criminale, dove veniva allegato un .PDF del tutto simile all'originale, ma con IBAN modificato e, naturalmente, diverso da quello originario del fornitore.
5) Il cliente, avendo ricevuto una doppia e-mail con la fattura della fornitura in allegato, rispondeva alla mail chiedendo al fornitore "Anna" se poteva procedere al pagamento o se avesse dovuto attendere eventuali ulteriori modifiche.
6) Il Cyber-Criminale rispondeva alla mail del cliente, spacciandosi per il fornitore "Anna", confermando che poteva procedere al pagamento come da ultima e-mail trasmessa (quella con l'IBAN modificato).

A fianco riportiamo la Timeline degli eventi a seguito dell'analisi da parte del C.R.A.M. di TG Soft.



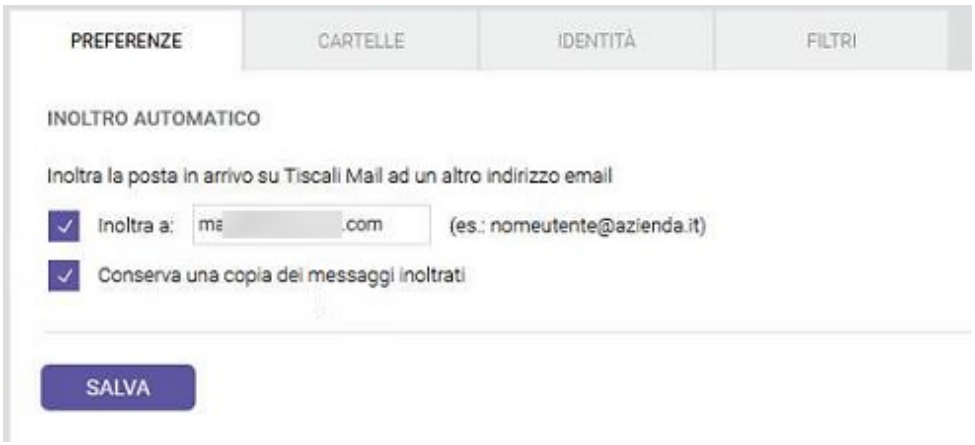
Fase di ANALISI del software di gestione della POSTA ELETTRONICA della VITTIMA

Grazie all'analisi delle email il C.R.A.M. di TG Soft ha individuato che il problema era localizzato nella casella di posta del fornitore, cioè nel PC di "Anna".

Accedendo quindi alla casella di posta elettronica del fornitore, purtroppo, vi è stata la conferma di quanto, fino a quel momento, si presumeva.

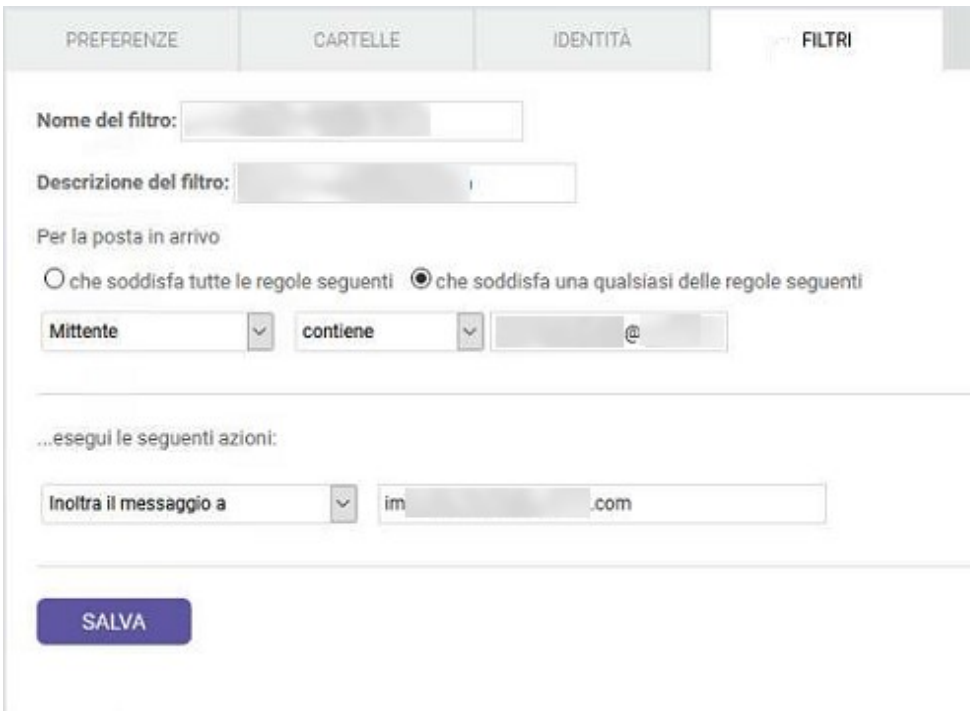
All'accesso della casella di posta nelle impostazioni si riscontravano due diversi inoltri, come di seguito evidenziato:

⇒ il primo inoltro configurato era impostato per inviare tutte le mail che riceveva il fornitore ad un altro account di posta (account email del Cyber-Criminale), mantenendone una copia nella casella di posta del fornitore "Anna" così da non destare sospetti ==>



⇒ il secondo inoltro invece è molto diverso dal primo ed era stato strutturato per poter "seguire" la conversazione tra il fornitore e il cliente. Questo tipo di configurazione nei filtri della casella di posta, permetteva l'inoltro di tutte le mail che venivano inviate al cliente dal fornitore.

Infatti nella regola del filtro era impostato che se nella voce mittente era presente l'indirizzo email del cliente una copia di questa mail veniva inviata anche ad un altro indirizzo email, anch'esso del Cyber-Criminale. Qui di seguito l'estratto della schermata interessata:



Fase di ANALISI del COMPUTER della VITTIMA

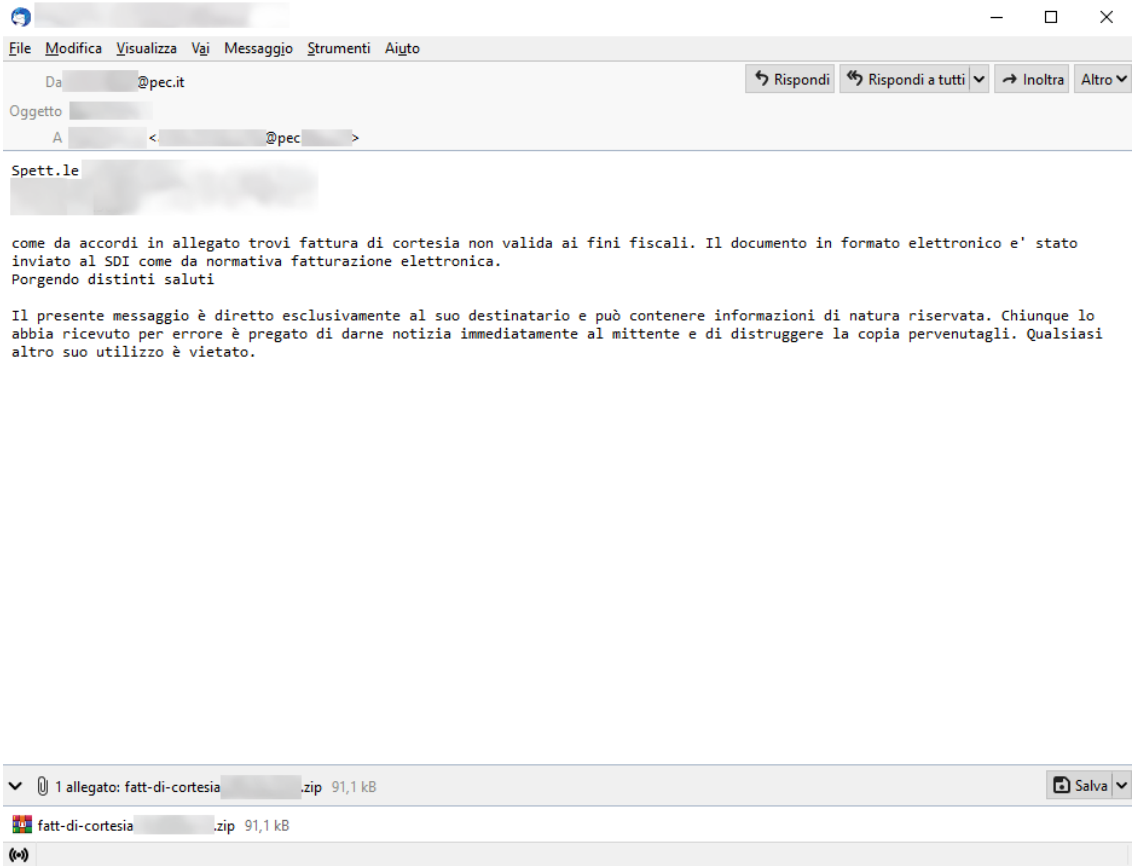
Si è poi passati ad analizzare la postazione di lavoro del fornitore, dove si riscontrava la presenza di malware Trojan della famiglia **sLoad**. Questo tipo di malware ha tra le sue peculiarità quella di rubare le credenziali di accesso a vari servizi tra cui anche quello della casella di posta elettronica.

Il malware utilizza vari programmi di sistema per eseguire le sue operazioni, sfrutta tool come, ad esempio: *bitsadmin* e *powershell* per eseguire le parti del suo codice malevolo e rimanere quindi attivo, ovvero mantenere la sua persistenza.

La distribuzione del Trojan **sLoad** avviene normalmente tramite account di posta elettronica compromessi, gli account di posta elettronica per lo più utilizzati sono però quelli PEC (posta elettronica certificata) che fa presumere agli ignari riceventi che questo tipo di email siano più sicure a livello di protezione malware.

Questo convincimento rende molte persone più propense ad aprire email PEC portandole a dare meno peso a quanto scritto all'interno e a sentirsi più sicure per quanto riguarda anche gli allegati presenti all'interno dell'email stessa.

Qui di seguito riportiamo un esempio di email inviata tramite un account PEC compromesso, che veicola il Trojan **sLoad** in una delle sue varie campagne mensili:



Come si può notare nell'immagine, nel corpo del messaggio vi è un testo ben strutturato con all'inizio intestazione aziendale accurata in base all'indirizzo e-mail al quale viene inviato e il testo ben scritto.

Può essere molto difficile presumere che l'e-mail sia una truffa.

In allegato alla e-mail di esempio troviamo un file ZIP che ha come nome fatt-di-cortesia[PIVA].zip dell'azienda interessata. Chi aprirà poi l'allegato compresso troverà al suo interno un altro file zippato che se anch'esso estratto avrà al suo interno un file con stesso nome del primo file ma con estensione WSF. Se si dovesse eseguire il file WSF verrebbe avviato il download del payload del malware e la sua installazione con anche la persistenza nel computer della vittima.

CONCLUSIONI

sLoad è un malware che viene veicolato via posta elettronica attraverso campagne di malspam MIRATE. L'email infetta è indirizzata ad una specifica AZIENDA, dove il corpo del messaggio contiene informazioni inerenti all'azienda da colpire, come nome della società, indirizzo, partita iva o codice fiscale.

Il FORNITORE che abbiamo chiamato con il nome di fantasia "ANNA" è stato scelto da sLoad come vittima a cui perpetrare l'attacco informatico, rubando le credenziali della casella di posta elettronica per poi dirottare il bonifico del CLIENTE verso il conto corrente del cyber-criminale.

E' stato possibile ricostruire nei minimi dettagli l'attacco informatico subito dal FORNITORE che ha portato nelle successive settimane al dirottamento del bonifico a favore del cyber-criminale.

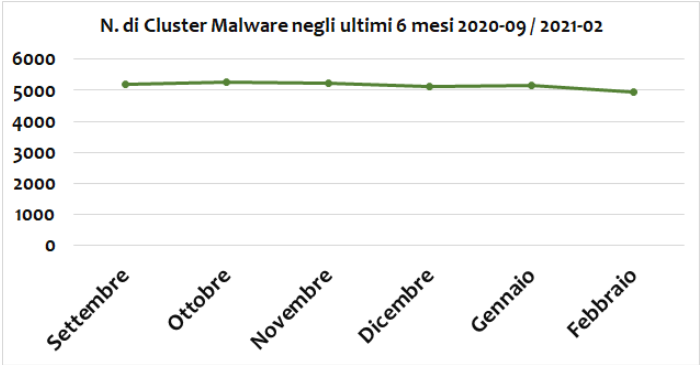
Se anche tu hai subito un attacco informatico di tipo RANSOMWARE, una FRODE informatica (dirottamento bonifico/i) oppure hai ricevuto email sospette, **TG Soft** Cyber Security Specialist mette a disposizione la propria organizzazione, grazie ai suoi Ricercatori ed Analisti di provata e consolidata esperienza in queste attività di estrema specializzazione, nel supportare al meglio qualsiasi azienda PMI come anche grandi aziende nelle attività di INCIDENT RESPONSE per individuare le cause dell'attacco e mettere in sicurezza l'azienda stessa.

Statistiche Malware

Febbraio 2021 — ITALIA

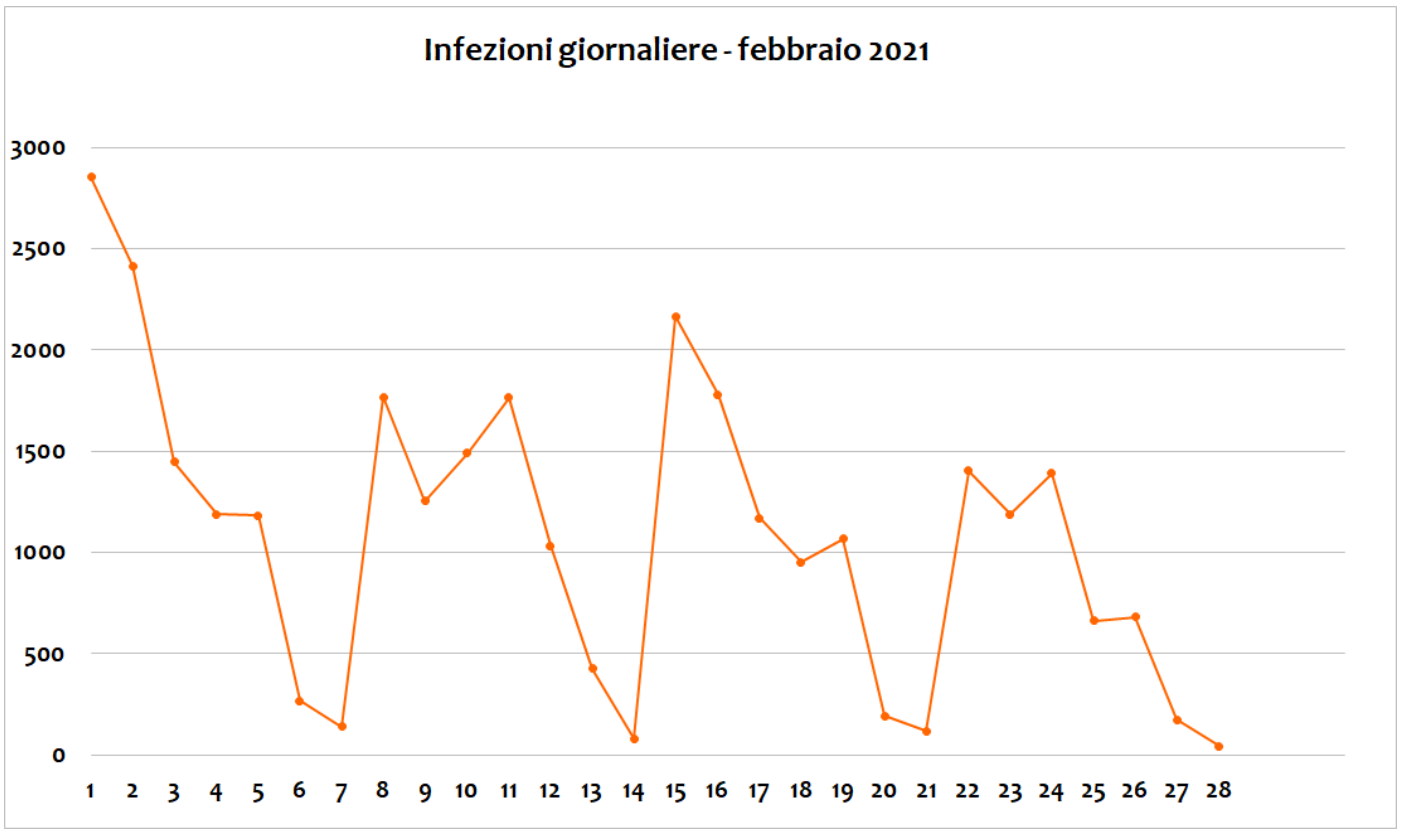
I dati della telemetria del C.R.A.M. di TG Soft sono raccolti dagli utenti che utilizzano il software antivirus Vir.IT eXplorer. Le segnalazioni derivano da attacchi bloccati oppure malware riscontrati all'interno del parco macchine monitorato. Ogni minaccia identificata da Vir.IT eXplorer viene classificata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

Nel mese di febbraio , il numero di cluster rilevato è sceso sotto la soglia delle 5000 unità, precisamente 4958 con un delta negativo rispetto a gennaio di 184 unità (-3,58%) che potrebbe apparire come una riduzione ma se andiamo a confrontare tale riduzione con il numero ridotto di giorni di febbraio (28) rispetto a gennaio (31) che percentualmente rappresenta un –9,68%, si può concludere che le infezioni di febbraio proporzionalmente sono state maggiori di quelle di gennaio 2021.



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

La prima settimana di febbraio è iniziata con un dato molto alto e tipico di inizio mese (oltre 2500 infezioni). Nei successivi lunedì i picchi di inizio settimana hanno sempre superato quota 1500 ma mai quota 2500 come ad inizio mese. Nei fine settimana invece, le rilevazioni sono tutte scese sotto le 500 unità. Da notare il dato del'11 e del 24 febbraio che evidenzia un marcato picco infrasettimanale.



Nel grafico sottostante vediamo le statistiche relative al mese di febbraio 2021 suddivise per "Tipologia Malware" riscontrate in Italia.

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

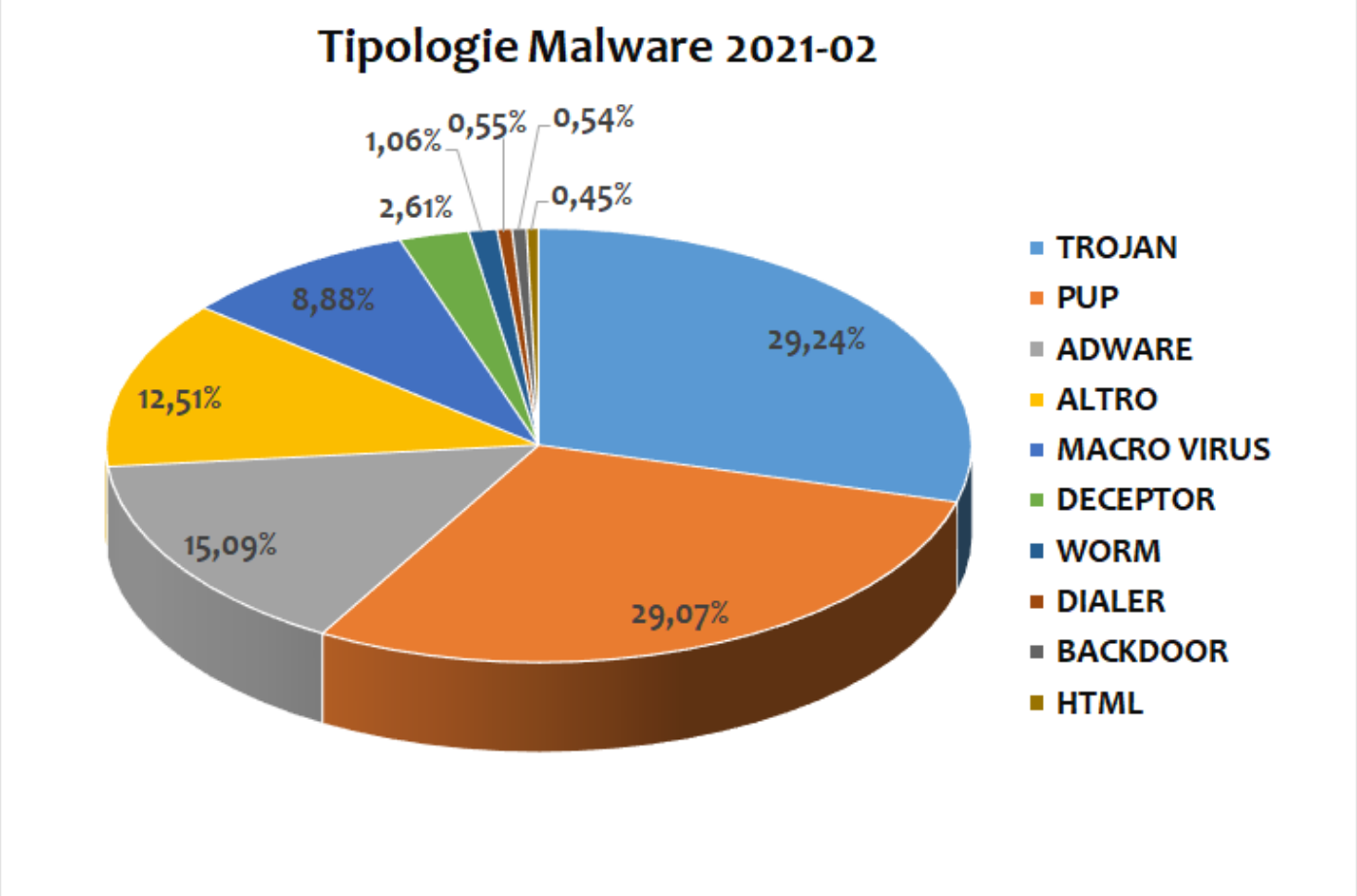
I malware si suddividono in diverse tipologie: Adware, Backdoor, Trojan, Worm, Virus, PUA/PUP, Deceptor, etc.

Nel mese di febbraio **TROJAN** (29,24%) e **PUP** (29,07%) salgono oltre i 29 punti percentuali, entrambi guadagnano circa un punto rispetto a gennaio (Trojan +1,07% - PUP +0,93%). Al terzo posto, stabili, gli **ADWARE** con il 15,09% (-1,43%). Scivolano al quinto posto con un vistoso calo di circa 3 punti percentuali i **MACRO VIRUS** (8,88%) lasciando la quarta piazza alla categoria ALTRO (12,51%). La flessione dei MACROVIRUS è probabilmente la conseguenza dello smantellamento della Botnet di Emotet che anche a gennaio avevano alterato questo valore oltre i 10 punti percentuali.

Confermata la sesta posizione per i **DECEPTOR** con il 2,61% (+0,93%) e la settima per gli WORM con lo 1,06% (+0,2%) seguono **DIALER** (0,55%), **BACKDOOR** (0,54%). Chiude la classifica la categoria **HTML** con lo 0,45%.

TROJAN, PUP e ADWARE compongono il podio del mese, assieme coprono oltre il 73% delle infezioni di febbraio.

I TROJAN si consolidiano in prima posizione, 2° e 3° posizione per PUP ed ADWARE che nell'insieme coprono quasi i 3/4 delle infezioni di febbraio



Analizziamo le statistiche di febbraio dei singoli Malware. Anche questo mese si riconferma al primo posto il **PUP.Win32.MindSpark.F** con il 5,68% delle infezioni, che può compromettere il tuo browser, modificando l'home page e il motore di ricerca. Un altra pericolosa minaccia che segue le orme di MindSpark è il **PUP.Win32.InstallCore.C** che a febbraio entra nella TOP10 e si insedia in seconda posizione con il 4,35%.

Al terzo posto e in netto calo causato dallo stop di EMOTET, troviamo **Office.VBA_Macro_Heur** (tipologia MACRO VIRUS) con il 2,35% (dal 4,70% di gennaio).

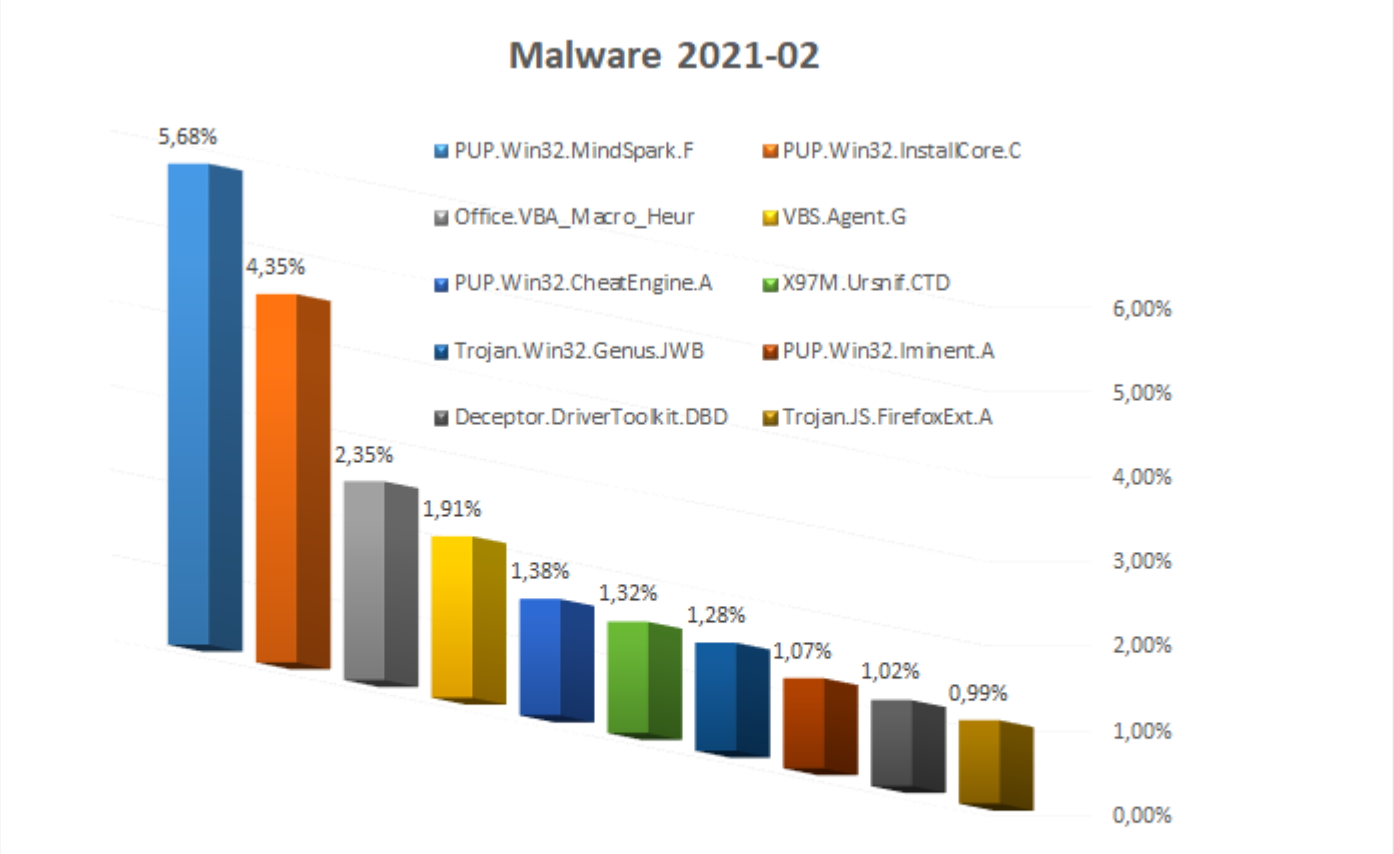
Si tratta di un dato ottenuto tramite l'analisi euristica e riguarda i file contenenti macro potenzialmente pericolose di diverse famiglie di malware.

Fuori podio nella TOP10 di febbraio troviamo in quarta posizione **VBS.Agent.G** (1,91%), tra i PUP compaiono in quinta e ottava posizione rispettivamente **PUP.WIN32.CheatEngine.A** e **PUP.Win32.Iminent.A**. Tra i Trojan troviamo in settima e decima posizione rispettivamente **Trojan.Win32.Genus.JWB** e **Trojan.JS.FirefoxExt.A**.

Al sesto posto con l'1,32% troviamo **X97M.Ursnif.CTD** che identifica le minacce, in questo caso il noto UrSnif, scatenate all'apertura delle macro all'interno dei file xls. In nona posizione anche un deceptor, si tratta di **Deceptor.DriverToolkit.OBD** software che propone il rinnovo dei driver nel sistema operativo in cui viene eseguito.

I MALWARE della TOP10 rappresentano il 21,35% delle infezioni di febbraio, il rimanente 78,65% è dato da altri 4948 cluster di malware.

Nella Top10 troviamo 4 tipologie differenti di PUP, 2 tipologie di Trojan, e 2 tipologie di Macro Virus. Con una sola presenza compaiono i Deceptor e la categoria Altro. Da notare che nella Top10 di febbraio non vi sono elementi della tipologia Virus.



Statistiche Malware via email

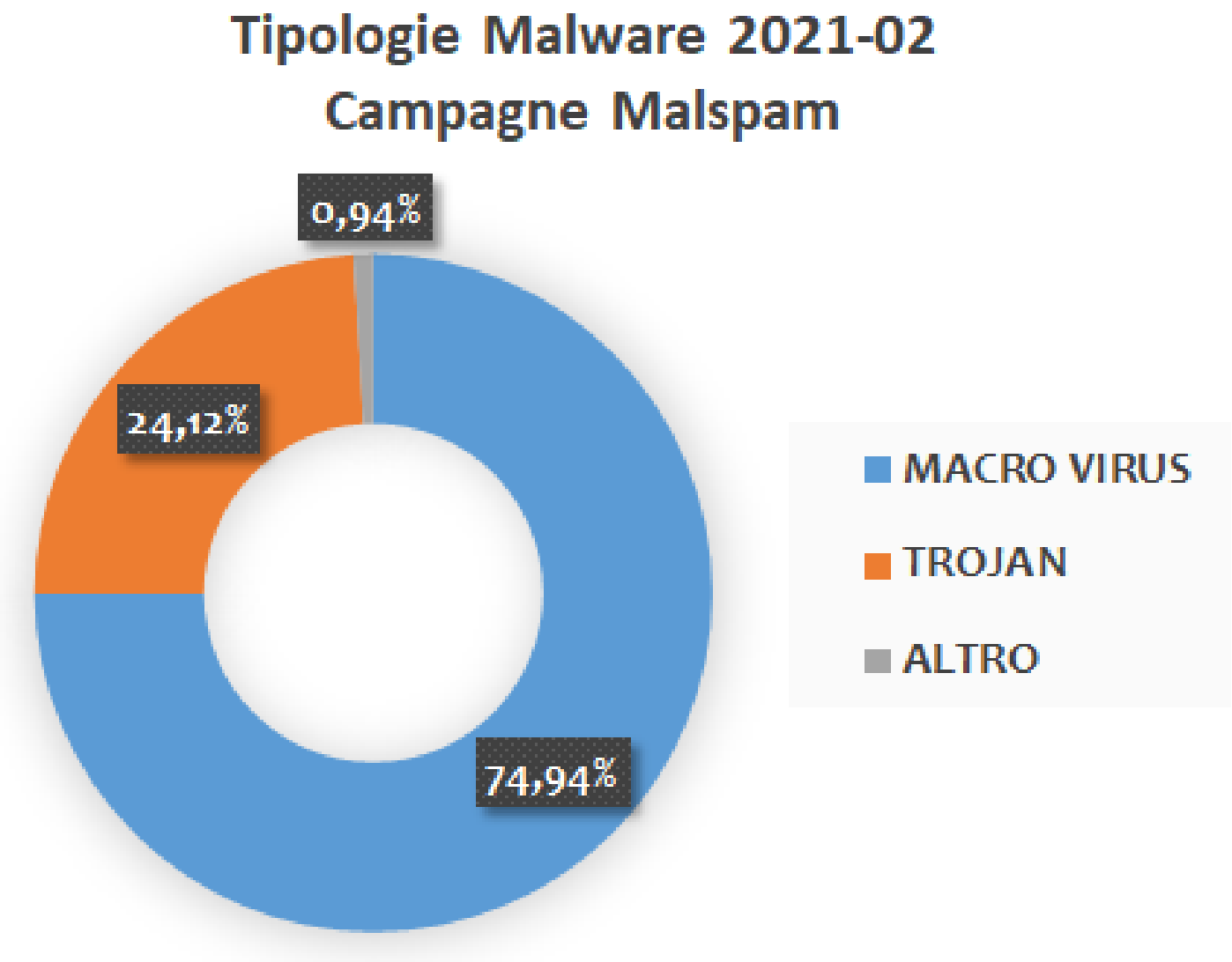
Febbraio 2021 - ITALIA

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

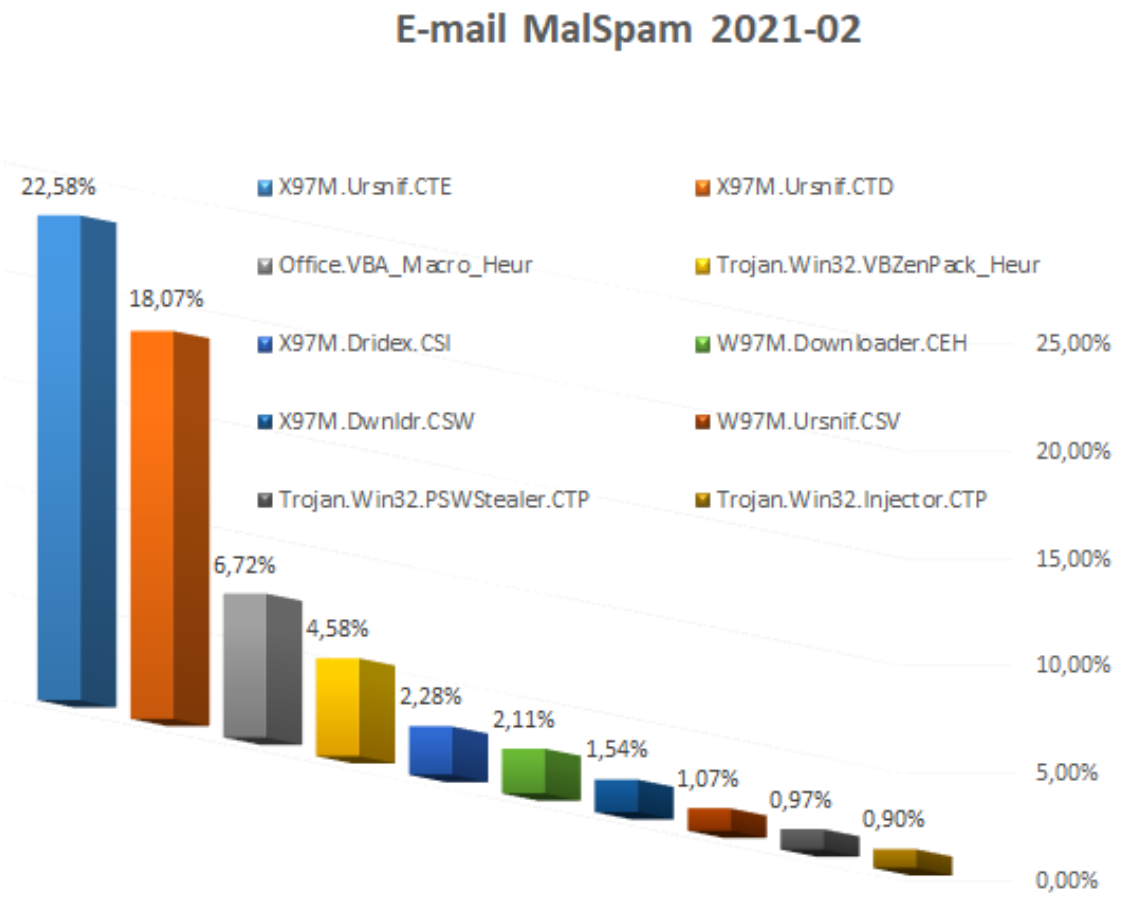
La categoria dei **MACRO VIRUS** detiene anche per il mese di febbraio la prima posizione con il 74,94%, in leggero aumento (+1,69%) rispetto al mese di gennaio.

Al contrario, l'altra macro categoria nella quale di norma ricadono una grossa parte dei malware veicolati tramite mail, quella dei **TROJAN**, scende del 1,66% con un 24,12% totale.

Le rimanenti campagne (che includono varie famiglie come WORM e BACKDOOR) sono state invece raggruppate al terzo posto nella macro categoria ALTRO, rappresentando solo il 0,94% delle campagne totali.



Analizzando le statistiche delle campagne di malspam per singolo malware, al primo posto troviamo X97M.Ursnif.CTE con il 22,58%, che ricade nella famiglia dei MACRO VIRUS (vedi grafico precedente), in particolare riguarda i file Excel contenenti macro infette. Allo stesso modo, la seconda posizione viene ricoperta da un altro malware appartenente alla famiglia dei MACRO VIRUS , l'X97M.Ursnif.CTD, ovvero il famigerato trojan bancario UrSnif, mantenendo così la seconda posizione rispetto al mese di gennaio, ma nella variante .CTD con il 18,07%.



Chiude la Top 3 al terzo posto la più generica categoria **Office.VBA_Macro_Heur**, sempre della famiglia dei MACRO VIRUS, in "caduta" dal 1°a l 3° posto rispetto al mese precedente co il 6,72% (a gennaio si era in vetta con ampio margine con il 35,88%).

Le altre posizioni ricoperte da malware appartenenti alla famiglia dei MACRO VIRUS vanno dalla 5° all'8° posizione, tra cui la 5° ricoperta dal malware **X97M.Dridex.CSI** con il 2,28% e l'8° ricoperta dal malware **W97M.Ursnif.CSV**, un tipo di documento Word contenente una macro che va ad installare il Trojan Banker UrSnif.

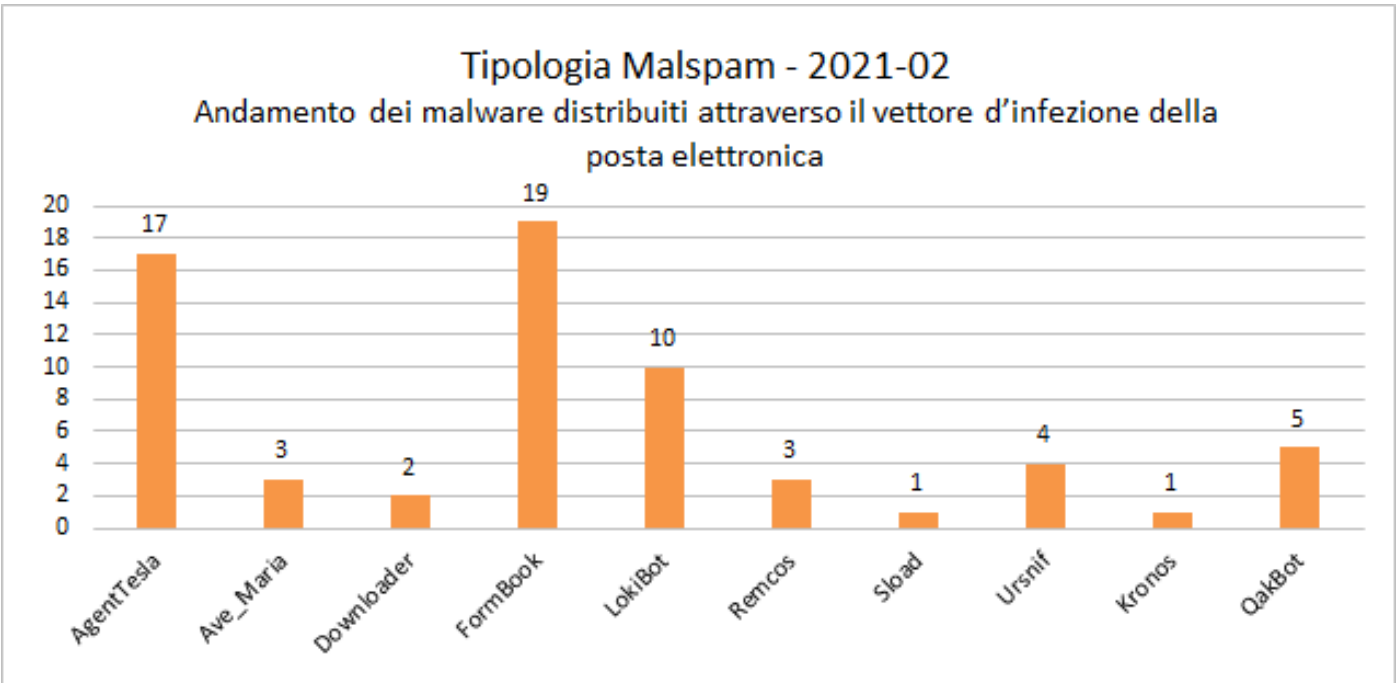
Il primo trojan lo troviamo solo in quarta posizione, in particolare il **Trojan.Win32.PSWStealer.CRR**, con il 4,58%. Gli altri due trojan, il Trojan.Win32.PSWStealer.CTP e il Trojan.Win32.Injector.CTP, chiudono la classifica con lo 0,97% e lo 0,90% rispettivamente.

Complessivamente, raffrontando il mese di gennaio e l'attuale mese di febbraio, nella TOP10 di gennaio ricadono un totale di 277 campagne malspam (il 68,48% del totale), mentre nella TOP10 di febbraio ricadono un totale di 380 campagne di malspam (il 60,82% del totale), a riprova dell'aumento delle campagne massive di malspam registrato nel mese (+27%).

Analisi dei malware di febbraio

Nel mese di febbraio in Italia, attraverso le campagne di malspam che hanno "targettizzato" l'utenza italiana (email scritte in lingua italiana), sono stati veicolati 10 differenti tipologie di malware.

Nella figura sottostante possiamo vedere l'andamento dei malware distribuiti attraverso le mail nel mese di febbraio.



Se tralasciamo il famigerato malware Emotet, la cui rete è stata smantellata durante un'operazione congiunta di polizia tra il 25 e il 27 gennaio scorso, possiamo asserire che il mese di febbraio ha visto un considerevole aumento nel numero di campagne italiane distribuite (ad esempio il numero di email con allegato un sample del malware **AgentTesla** a gennaio era solamente 6, contro le 17 rilevate durante il mese di febbraio).

Il numero totale di mail rivolte all'utenza italiana questo mese è stato di 65 campagne malspam:

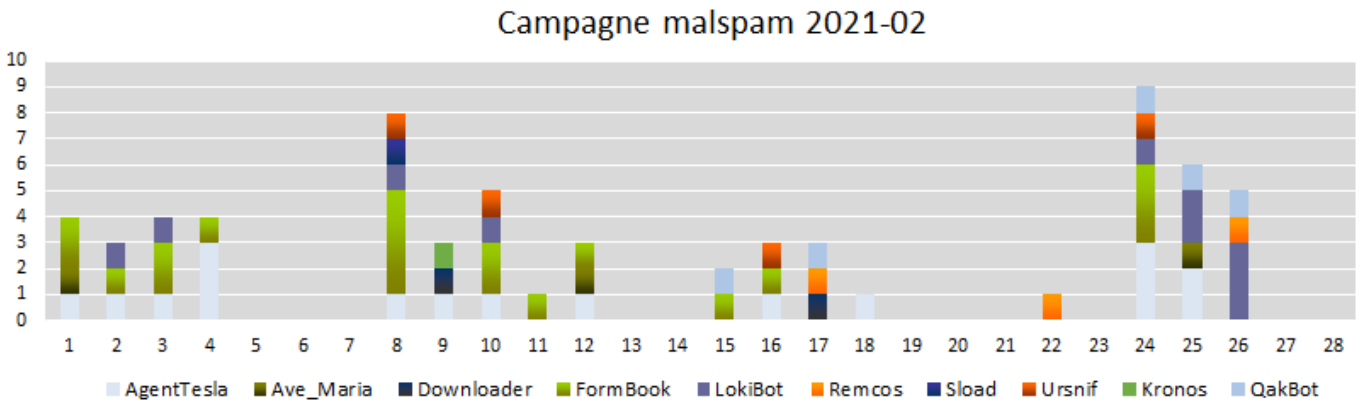
⇒ **19** campagne veicolavano **Formbook**, un RAT utilizzato per prendere controllo del computer della vittima per perpetrare azioni tra cui l'esfiltrazione delle password;

⇒ **17** invece sono state le campagne malspam (email con allegato malevolo) che infettavano il pc con **AgentTesla**, un altro famoso RAT molto in voga tra i criminali informatici.

⇒ numerose anche le campagne del trojan bancario **Lokibot**, che si attesta al terzo posto con **10** campagne (3 in più rispetto al mese precedente, nel quale però dato il minor numero di campagne diffuse si era comunque piazzato al secondo posto).

Altro malware degno di menzione è l'**Ursnif** (vedi paragrafo dedicato), un altro trojan bancario che nel mese di febbraio è stato diffuso con 4 campagne dedicate (ad es. a tema Ministero dello Sviluppo Economico). Il mese precedente era stato diffuso con 6 campagne.

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



A colpo d'occhio la costante giornaliera del mese di febbraio sembra essere il malware RAT AgentTesla, che con le sue 17 campagne è stato distribuito uniformemente con quasi 1 campagna al giorno. Lo stesso vale per il malware Formbook, ma fino alle terza settimana del mese compresa, in quanto la quarta ha visto solo un exploit nella giornata di mercoledì 24 con 3 campagne, 2 a tema "Pagamenti" mentre una a tema "Preventivi" (altra giornata prolifera per il Formbook è stata la giornata dell'8 febbraio con 4 campagne diffuse).

Ursnif invece presente con 1 campagna a settimana, ad eccezione della prima nella quale non sono state riscontrate campagne del noto password stealer bancario.

Le giornate 8 e 24 febbraio sopra menzionate corrispondono anche alle giornate a maggior concentrazione di malspam, rispettivamente con 8 e 9 campagne inviate all'utenza italiana. Rispetto al mese di gennaio si tratta di un calo, in quanto anche grazie alle numerose campagne di Emotet, si era registrato un picco di 16 campagne (15 delle quali per l'appunto di Emotet).

Per fare invece una media giornaliera delle campagne di malspam inviate all'utenza italiana, 4 giornate a parte dove troviamo solo 1 campagna, la media si attesta attorno alle 3 / 4 campagne distinte al giorno (in linea con il mese di gennaio).

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

Week 05 ==> dall'1 febbraio al 7 febbraio

Week 06 ==> dall'8 febbraio al 14 febbraio

Week 07 ==> dal 15 febbraio al 21 febbraio

Week 08 ==> dal 22 febbraio al 28 febbraio

Ursnif

Analisi delle campagne di febbraio

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

Come abbiamo visto, questo malware è uno dei più diffusi via email in Italia ma, a febbraio, è stato veicolato attraverso solo 4 campagne di malspam distribuite nelle ultime 3 settimane del mese contro le 6 campagne di gennaio.

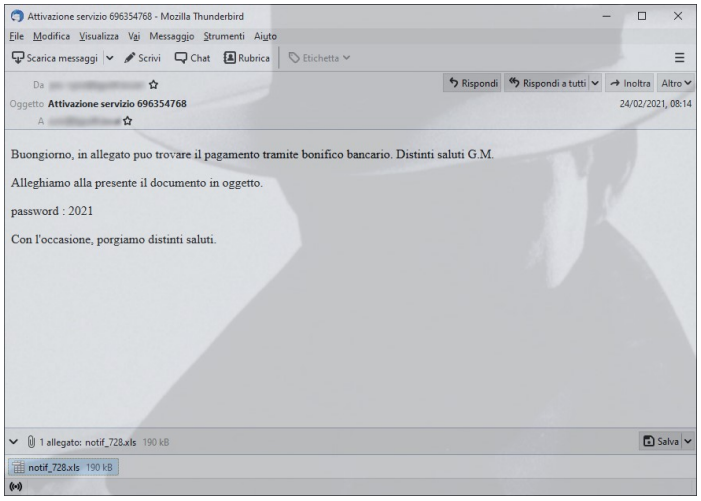
Come si può vedere dalla figura a fianco , le campagne sono presenti in tutte e tre le ultime settimane del mese solo la settimana dall'1 al 7 febbraio vede Ursnif assente.

Le principali campagne veicolate hanno sfruttato i seguenti temi:

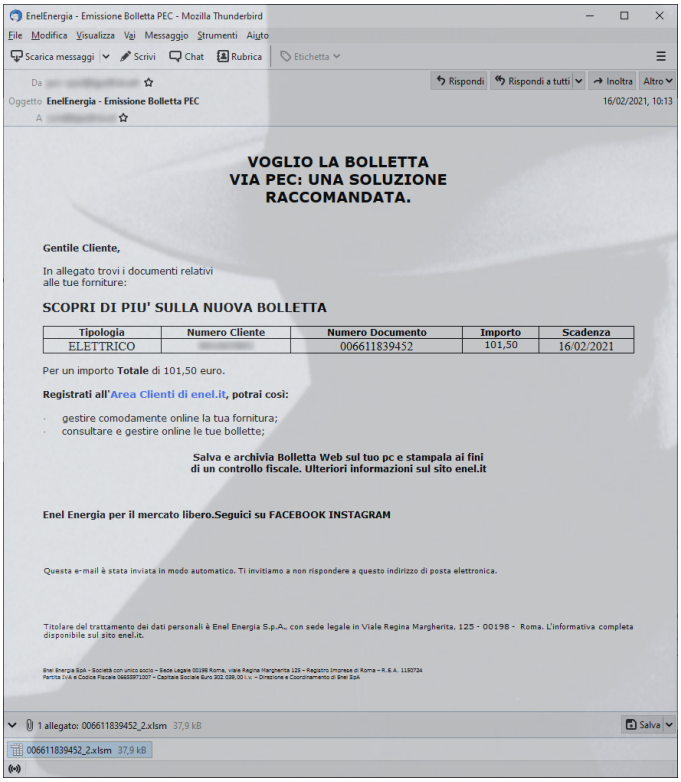
⇒ Ministero dello Sviluppo Economico (2)

⇒ Enel Energia (1)

⇒ Pagamenti - Attivazione servizio (1)



Dall'analisi delle campagne di malspam e dalle configurazioni individuate all' interno del trojan bancario Ursnif utilizzato , vi sono due gruppi distinti che hanno sfruttato questo malware a febbraio per attaccare l' utenza italiana. Entrambi i gruppi hanno veicolato due campagne di malspam , la prima con il tema condiviso Ministero dello Sviluppo Economico e la seconda rispettivamente a tema Enel energia ed un generico Pagamenti - Attivazione servizio.



Questi due gruppi cyber risultano essere attivi in italia da diversi mesi. Nei mesi scorsi abbiamo osservato il primo gruppo sfruttare temi istituzionali italiani come ad esempio l'Agenzia delle Entrate oppure il Ministero dello Sviluppo Economico come segnalato ed il secondo utilizzare come temi ordini o fatture collegati a società di spedizione come BRT (Bartolini), DHL oppure Enel Energia e/o Enigaseluce. Tuttavia nel mese di febbraio osserviamo i due gruppi veicolare entrambi una campagna a tema Ministero dello Sviluppo Economico nella seconda settimana del mese , ciononostante l'appartenenza a due gruppi distinti è osservabile dalla configurazione rilevata all' interno del malware utilizzato nelle campagne.

Ursnif è un malware bancario che punta a sottrarre denaro dal conto della vittima tramite il furto delle credenziali di accesso e l'intromissione nei pagamenti home banking attraverso un'injection nel browser.

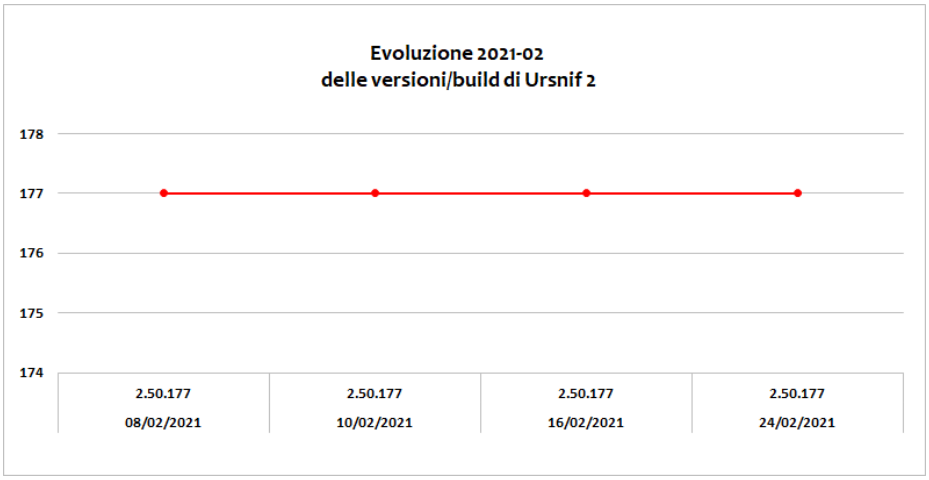
Gli allegati delle campagne di malspam veicolanti Ursnif cambiano spesso tipologia, nel mese di febbraio il tipo di allegato è stato variato in ogni campagna: un file zip contenente un file excel, un file word, un file excel e un file excel protetto da password.

I frequenti cambi, oltre a rendere più difficile per la vittima l' identificazione della mail fraudolenta, nei casi in cui viene utilizzata una password e/o una compressione sono atti a rendere più complicata l'identificazione dei file malevoli da parte dei software di protezione.

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 2020, entrambe le versioni, ma come negli scorsi mesi a febbraio è stata rilevata esclusivamente la versione 2. Nel mese di febbraio entrambi i gruppi hanno utilizzato la build 2.50.177 in tutte le campagne veicolate.

Ransomware

Febbraio 2021- ITALIA

Nel mese di febbraio 2021 si è registrato un andamento sostanzialmente costante degli attacchi Ransomware rispetto al mese di gennaio.

Dalla telemetria del modulo AntiRansomware protezione CryptoMalware integrato nella suite Vir.IT eXplorer PRO si sono riscontrati gli attacchi delle seguenti famiglie di ransomware:

⇒ **Phobos**

⇒ **Dharma**

⇒ **Sodinokibi (REvil)**

⇒ **LockBIT**

Gli attacchi rilevati nel mese di febbraio sono stati veicolati attraverso l'accesso abusivo al sistema **RDP** (Remote Desktop Protocol) di PC/SERVER esposti incautamente nella rete internet.

Una volta ottenuto l'accesso al sistema via RDP mediante il brute forcing delle credenziali, il CyberCriminale procede generalmente a:

⇒ RIMUOVERE le protezioni di sicurezza presenti

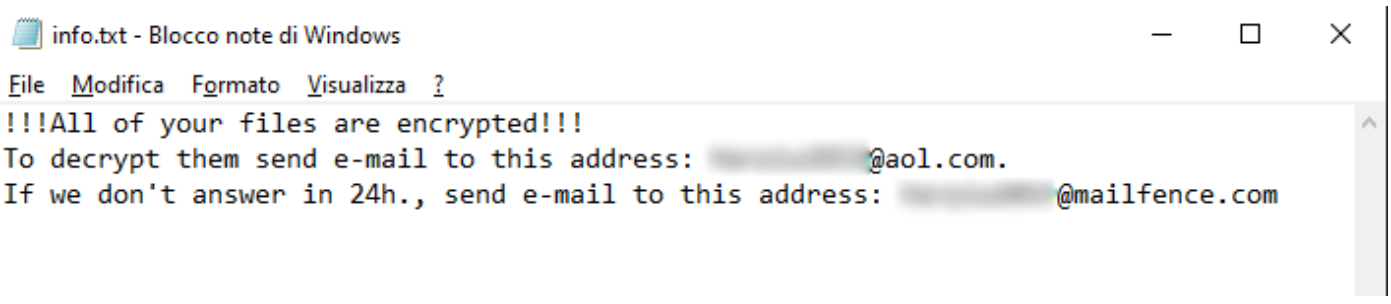
⇒ CANCELLARE i log di sistema

⇒ CANCELLARE le shadow copy di Windows se attive

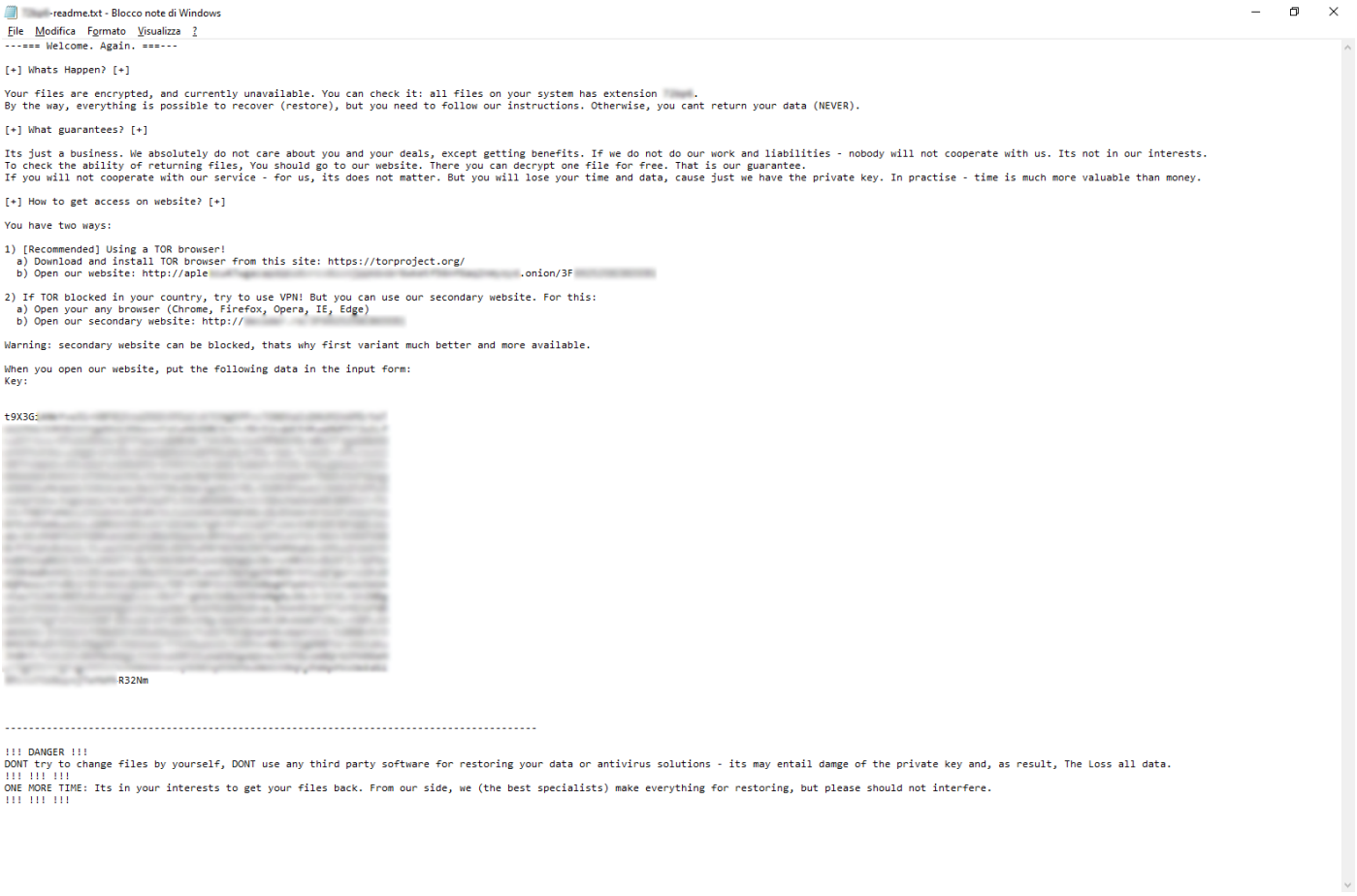
⇒ ESEGUIRE il Ransomware.

In attacchi più sofisticati i CyberCriminali, una volta ottenuto accesso al sistema, provvedono ad effettuare una scansione della rete interna per poi eseguire attività di spostamento laterale così da attaccare il maggior numero di PC/Server possibili.

Nelle figure di seguito possiamo vedere le istruzioni del riscatto del Ransomware **Phobos**



Nelle immagini successive vediamo le istruzioni del riscatto del ransomware Sodinokibi (REvil)



[redacted]-readme.txt - Blocco note di Windows

File Modifica Formato Visualizza ?

```
---=== Welcome. Again. ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it: all files on your system has extension [redacted].
By the way, everything is possible to recover (restore), but you need to follow our instructions. Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

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 not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website. There you can decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and data, cause just we have the private key. In practise - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site: https://torproject.org/
  b) Open our website: http://aple[redacted].onion/3F[redacted]

2) If TOR blocked in your country, try to use VPN! But you can use our secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: http://[redacted]

Warning: secondary website can be blocked, thats why first variant much better and more available.

When you open our website, put the following data in the input form:
Key:

t9X3G:
[redacted]
R32Nm

----------

!!! DANGER !!!
DONT try to change files by yourself, DONT use any third party software for restoring your data or antivirus solutions - its may entail damge of the private key and, as result, The Loss all data.
!!! !!! !!!
ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) make everything for restoring, but please should not interfere.
!!! !!! !!!
```

Come mi difendo dagli attacchi ransomware?

La minaccia ransomware è sempre più sofisticata ed aggressiva, il classico metodo delle firme antivirali non è completamente efficace per combattere queste tipologie di minacce vista la frequenza di aggiornamento e soprattutto la specificità del singolo attacco che spesso è "mirato" alla vittima rendendolo maggiormente "univoco".

E' fondamentale perciò dotarsi di una protezione di tipo Euristico-Comportamentale.

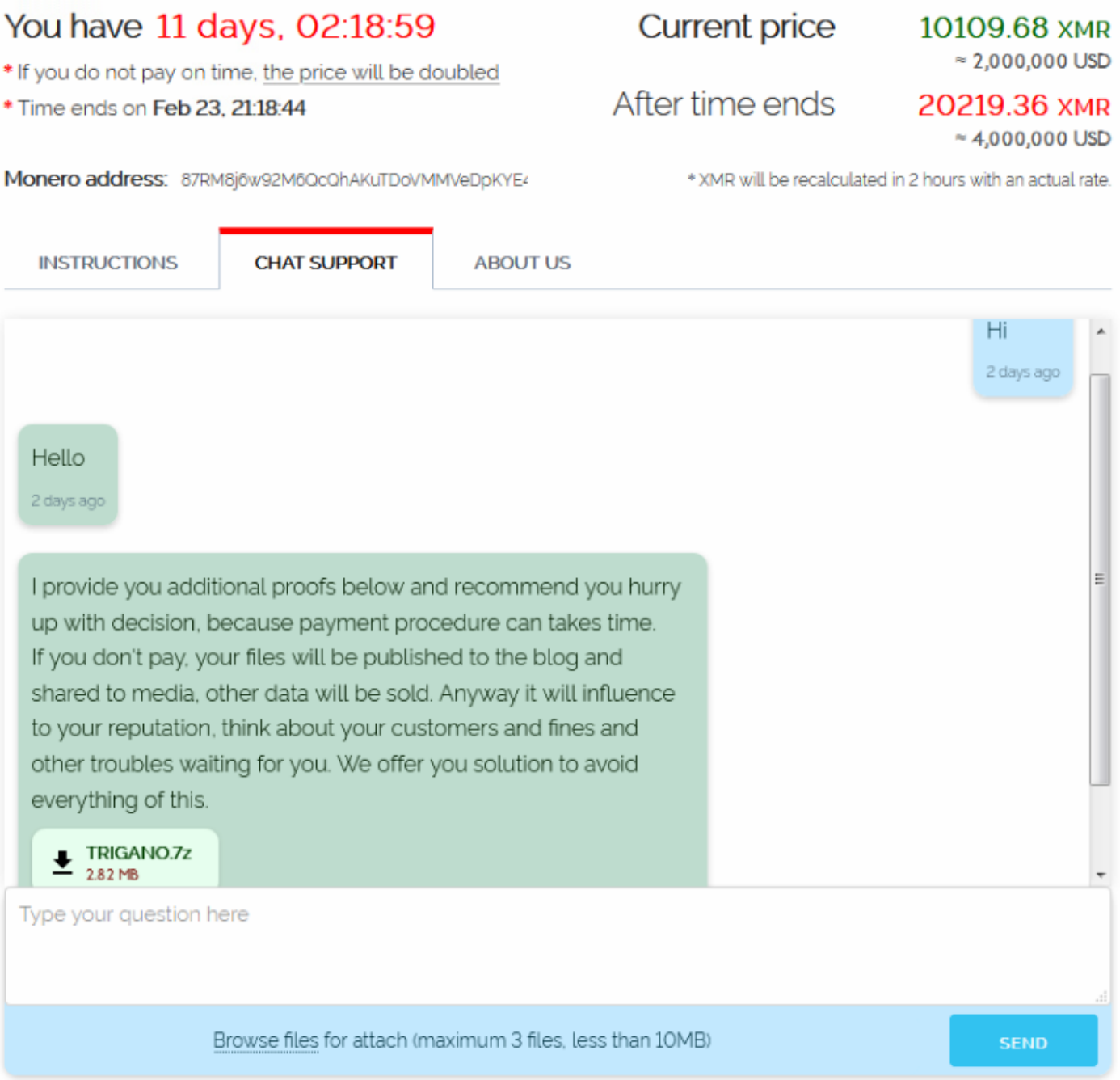
Il modulo AntiRansomware protezione CryptoMalware integrato nella suite **Vir.IT eXplorer PRO** include sofisticate tecnologie Euristico-Comportamentali, in grado di effettuare il monitoraggio in real-time degli accessi ai file del PC/Server rilevando e bloccando la cifratura dei dati in atto sia da processi eseguiti localmente sia da accessi avvenuti attraverso le condivisioni di rete.

Questa tecnologia permette di intervenire velocemente ed efficacemente anche in caso di minacce di nuova generazione o sviluppate ad-hoc per la vittima, salvaguardando i dati di PC/Server Windows(R).

A febbraio 2021 il gruppo CyberCriminale noto come **Sodinokibi** aka **REvil** ha attaccato la società francese Trigano. L'attività degli oltre 850 dipendenti della società, che ha sedi anche in Italia, è stata paralizzata dall'attacco.

Di seguito vediamo le immagini del sito per il pagamento del riscatto ai CyberCriminali dove è presente l'importo del riscatto, che ammonta a ben 2 milioni di dollari da pagare in BitCoin che successivamente raddoppieranno a 4 milioni di dollari, ed è presente inoltre un piccolo file di archivio contenente la dimostrazione dell'esfiltrazione dei dati:

Nella pagina successiva l'immagine della tab "CHAT SUPPORT"….



Come già segnalato la suite Vir.IT eXplorer PRO sarebbe stata, con ragionevolezza, in grado di segnalare tempestivamente l'attacco ed isolare la macchina/e dove questo è avvenuto e salvare dalla cifratura la maggior parte dei dati aziendali riducendo di molto il tempo di fermo delle attività non solo della macchina/e colpite dovute al loro ripristino ma anche delle attività aziendali a questa/e connesse grazie alle tecnologie:

⇒ Euristico-Comportamentali AntiRansomware protezione CryptoMalware;

⇒ di backup avanzate e specificatamente progettate per preservare i dati anche da attacchi Ransomware di nuova generazione.

Il gruppo CyberCriminale di Sodinokibi aka REvil ha inoltre pubblicato nel proprio Blog nel Dark Web la prova dell'esfiltrazione dei dati alla società italiana D.M. Barone SpA

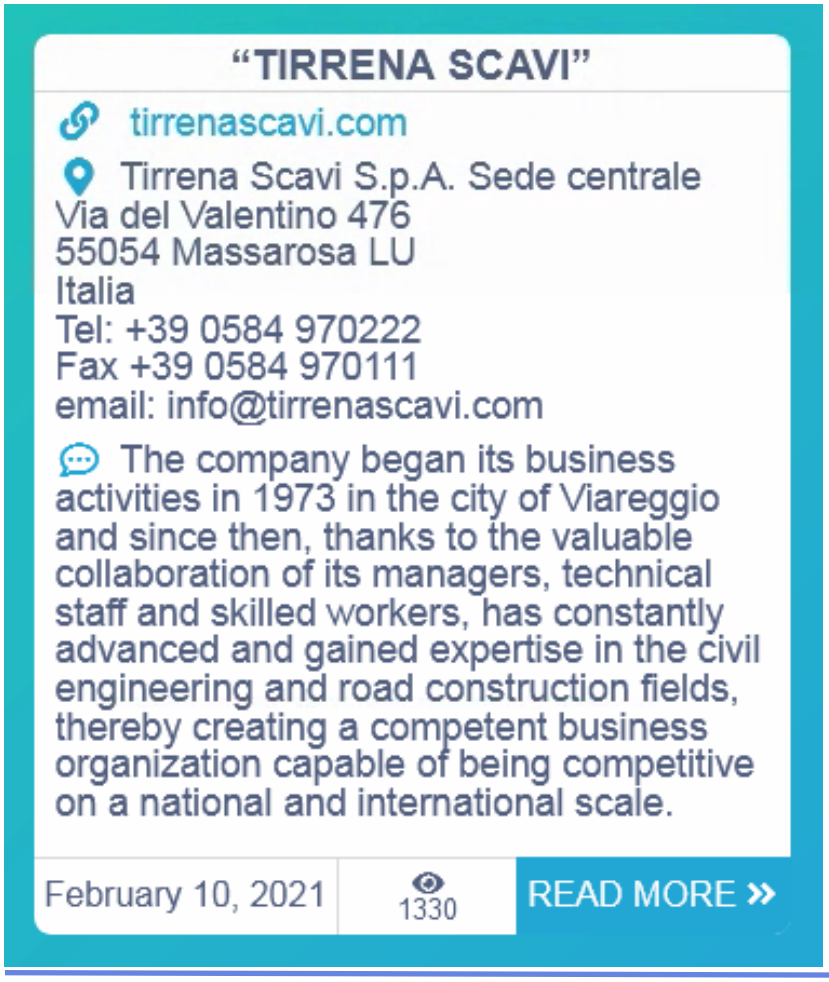
D.M. BARONE SPA

D.M. BARONE SPA
Health and Personal Care Wholesale
Modica, Ragusa, Italy

Employees: 123

Private Subsidiary • Headquarters
+39-0909438711 • www.dmbarone.com

[Untitled] (1).pdf	91 KB	12/12/
[Untitled].pdf	181 KB	11/28/
_1378.pdf	138 KB	7/9/20
_BOLLA_VAL_ (1).pdf	106 KB	7/13/2
_BOLLA_VAL_ .pdf	106 KB	7/10/2
_BOLLA_VAL_ .pdf	143 KB	7/9/20
~1791202.pdf	45 KB	12/3/2
~3332427.pdf	43 KB	3/3/20
~5927676 (1).pdf	49 KB	2/25/2
~5927676 (2).pdf	49 KB	2/25/2
~5927676 (3).pdf	49 KB	2/25/2
~5927676 (4).pdf	49 KB	2/25/2
~7377682.pdf	49 KB	7/3/20
~7650932.pdf	44 KB	4/1/20
~7937219 (1).pdf	45 KB	10/20/
~7937219.pdf	45 KB	10/20/
~7988055 (1).pdf	43 KB	11/10/
~7988055.pdf	43 KB	11/10/
~Do37A1.pdf	95 KB	7/28/2
~DoF4CA.pdf	90 KB	7/28/2
00_000096_2015_04_21_ITC.pdf	106 KB	4/28/2
000003 501.pdf	94 KB	6/16/2
4 ANNULLA e sostiuisce (1).pdf	92 KB	3/23/2
4 ANNULLA e sostiuisce .pdf	92 KB	3/23/2



"TIRRENA SCAVI"

tirrenascavi.com

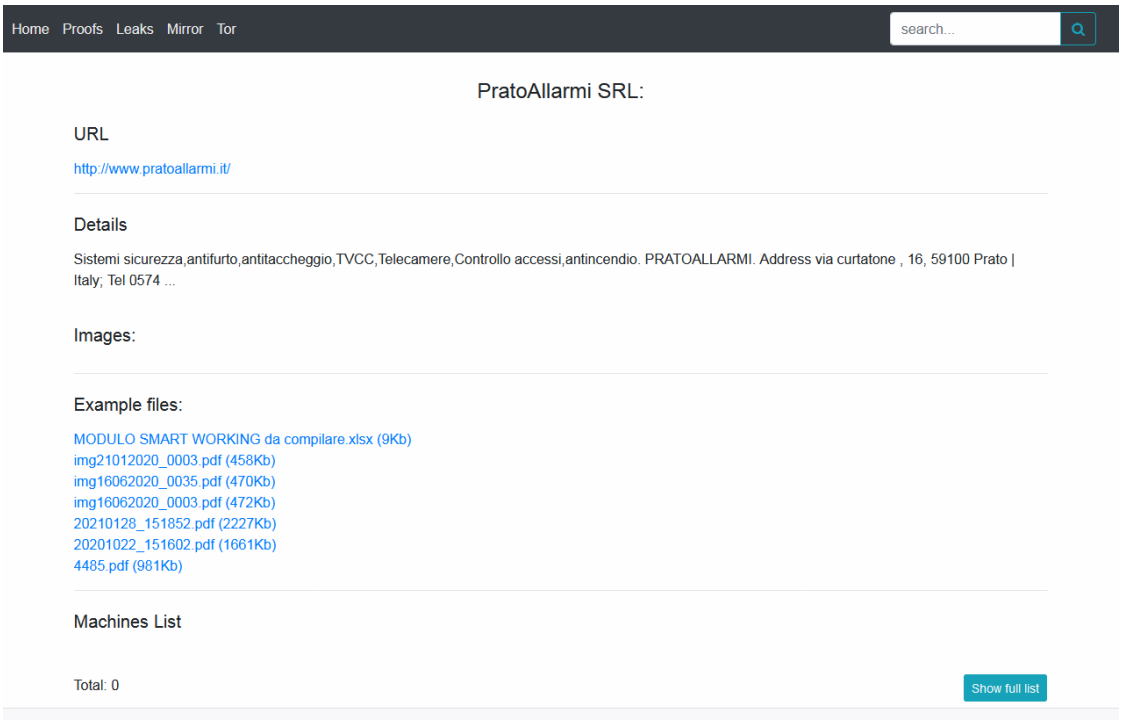
Tirrena Scavi S.p.A. Sede centrale
Via del Valentino 476
55054 Massarosa LU
Italia
Tel: +39 0584 970222
Fax +39 0584 970111
email: info@tirrenascavi.com

The company began its business activities in 1973 in the city of Viareggio and since then, thanks to the valuable collaboration of its managers, technical staff and skilled workers, has constantly advanced and gained expertise in the civil engineering and road construction fields, thereby creating a competent business organization capable of being competitive on a national and international scale.

February 10, 2021 | 1330 | READ MORE »

A febbraio anche il gruppo CyberCriminale alle spalle del Ransomware noto come CONTI miete vittime in Italia, rivendicando l'attacco alla società Tirrena Scavi S.p.A. nel proprio Blog nel Dark Web come vediamo dall'immagine a sinistra

Attivo anche il gruppo associato al ransomware **DoppelPaymer** che pubblica nel proprio Blog i dettagli dell'attacco alla società PratoAllarmi Srl:



Ultimo ma non ultimo, attivo anche in Italia, si abbatte prima su un'azienda di supporto informatico dell'Emilia che si "pregia" di offrire anche servizi di infoSec… e da questa attraverso la VPN utilizzata come canale preferenziale per effettuare attività di manutenzione da remoto il Ransomware dopo averne acquisto le credenziali di accesso abbatte anche anche alcune aziende cliente che hanno ritenuto opportuno richiederci attività consulenziale di IR (IncidentResponse) per fare luce sull'incidente.

Si è trattato di un'attacco da parte del Ransomware **LockBIT** che ha messo fuori combattimento la rete informatica costituita da circa 300 computer il cui rimessaggio ha impegnato i tecnici interni per circa una decina di giorni e ha rallentato conseguentemente anche tutte le attività di consegna ed amministrative.

Per altro anche questo attacco se l'azienda informatica avesse avuto in uso la suite **Vir.IT eXplorer PRO** avrebbe potuto essere bloccato nella fase iniziale dell'attacco sempre che ,su un PC/Server ove il ***Vir.IT eXplorer PRO*** fosse correttamente:

⇒ INSTALLATO;

⇒ CONFIGURATO;

⇒ AGGIORNATO;

⇒ UTILIZZATO.

Prevalenza

Febbraio 2021 — 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.

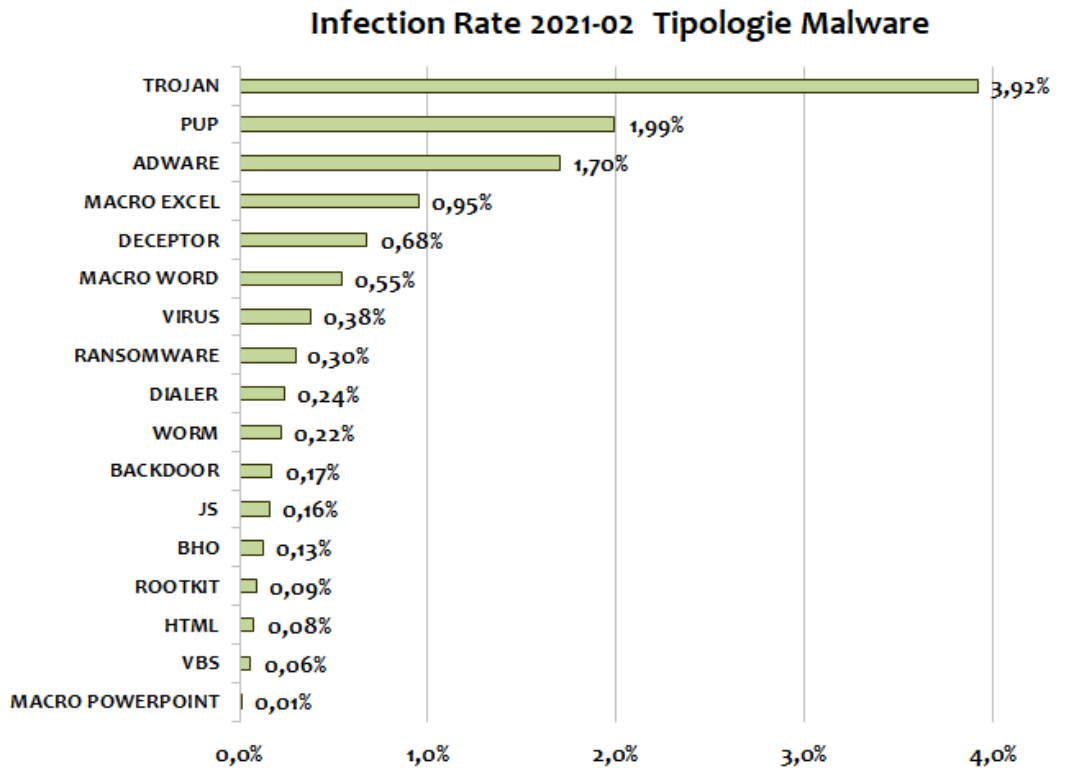
Vediamo ora i dati relativi alla prevalenza dei malware registrati dal C.R.A.M. di TG Soft nel mese di gennaio. Per prevalenza si intende l'incidenza che i malware hanno in un determinato periodo. Il valore calcolato si chiama "rate di infezione".

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)

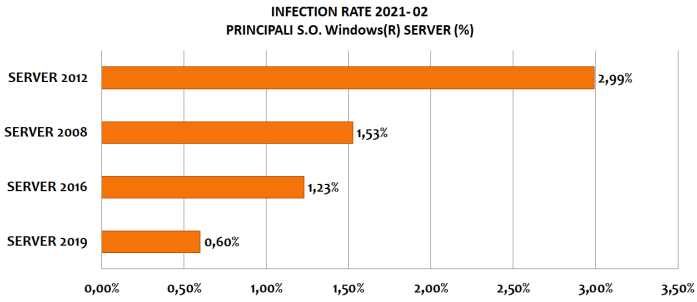
Si confermano ai primi due posti, nell'ordine, i **Trojan** con una percentuale del 3,92% e i **PUP** , con una percentuale dell'1,99%. Terzo gradino del podio per la categoria **Adware** con l'1,70%. In 4ª e 5ª posizione troviamo l**e MACRO EXCEL e DECEPTOR** in salita dalla 5ª e dalla 7ª posizione**.** In leggera salita i **VIRUS** (7° con lo **0,38%)** preceduti dai MACRO WORD in "caduta" dalla 4ª alla 6ª posizione. I **Ransomware** con lo 0,30% recuperano una posizione passando dalla 9° all'ottava piazza. 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, famoso ed oramai estinto FakeGDF (virus della polizia di stato, guardia di finanza etc.).



Andiamo ora ad analizzare la prevalenza delle infezioni del mese di febbraio 2021, in base ai sistemi operativi suddivisi tra sistemi Server e Client. Nelle immagini che seguono 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.

Analizzando prima i sistemi operativi SERVER, si conferma ancora che la probabilità dell'infezione/attacco ad un Server 2019 di ultima generazione rispetto ad un Server 2012 (più datato…) è di un ordine di grandezza inferiore, circa 0,60% contro 2,99%.

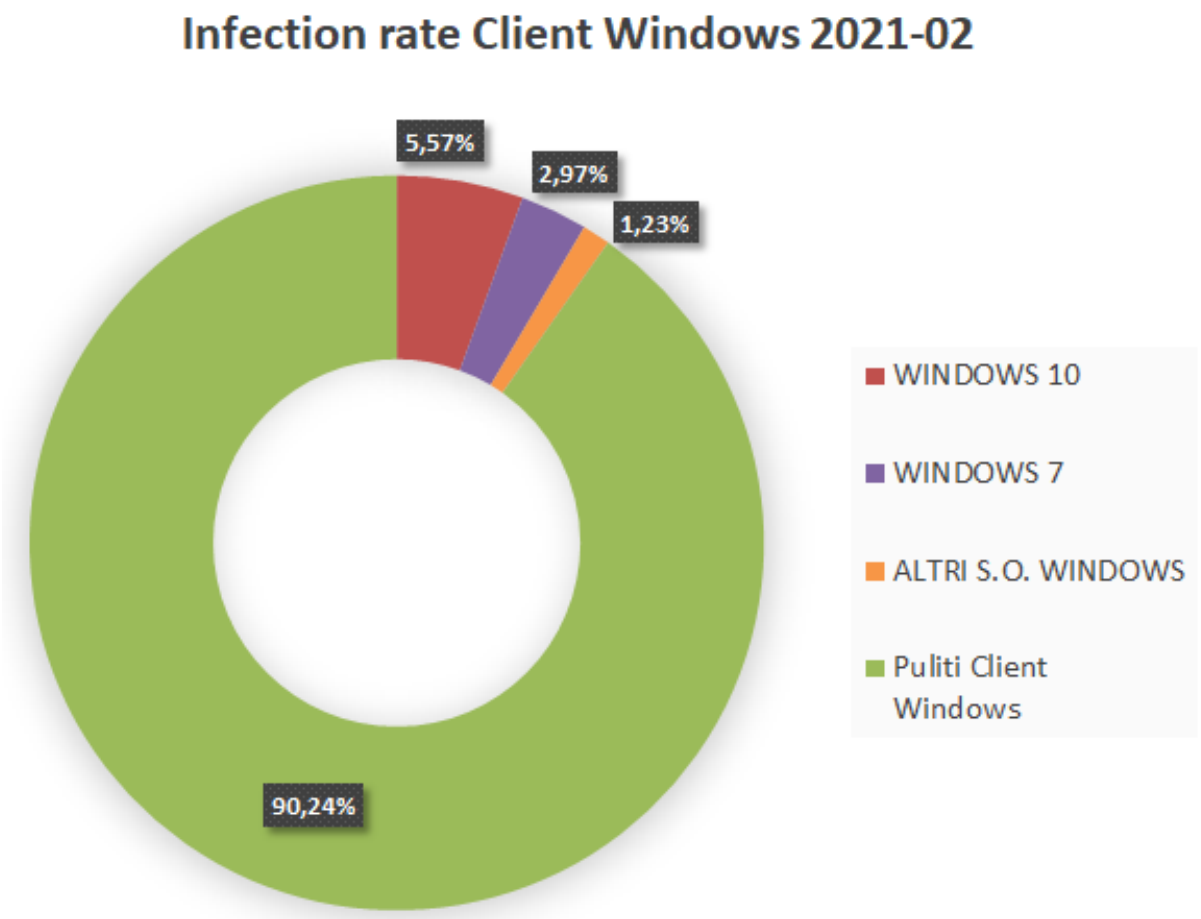
Nelle statistiche relative alla prevalenza delle infezioni dei computer client nel febbraio 2021 abbiamo riscontrato che il **9,77%** (contro il **10,30**% di gen-



nario) dei terminali è stato infettato o ha subito un attacco probabilmente dovuto anche al fatto che febbraio ha 28 giorni contro i 31 di gennaio.

Questo dato indica che poco meno di **10 computer su 100** sono stati colpiti da malware nel mese di febbraio. Nella figura sottostante possiamo vedere il grafico delle infezioni in base ai sistemi operativi dei Client, dove il campione analizzato è così composto:

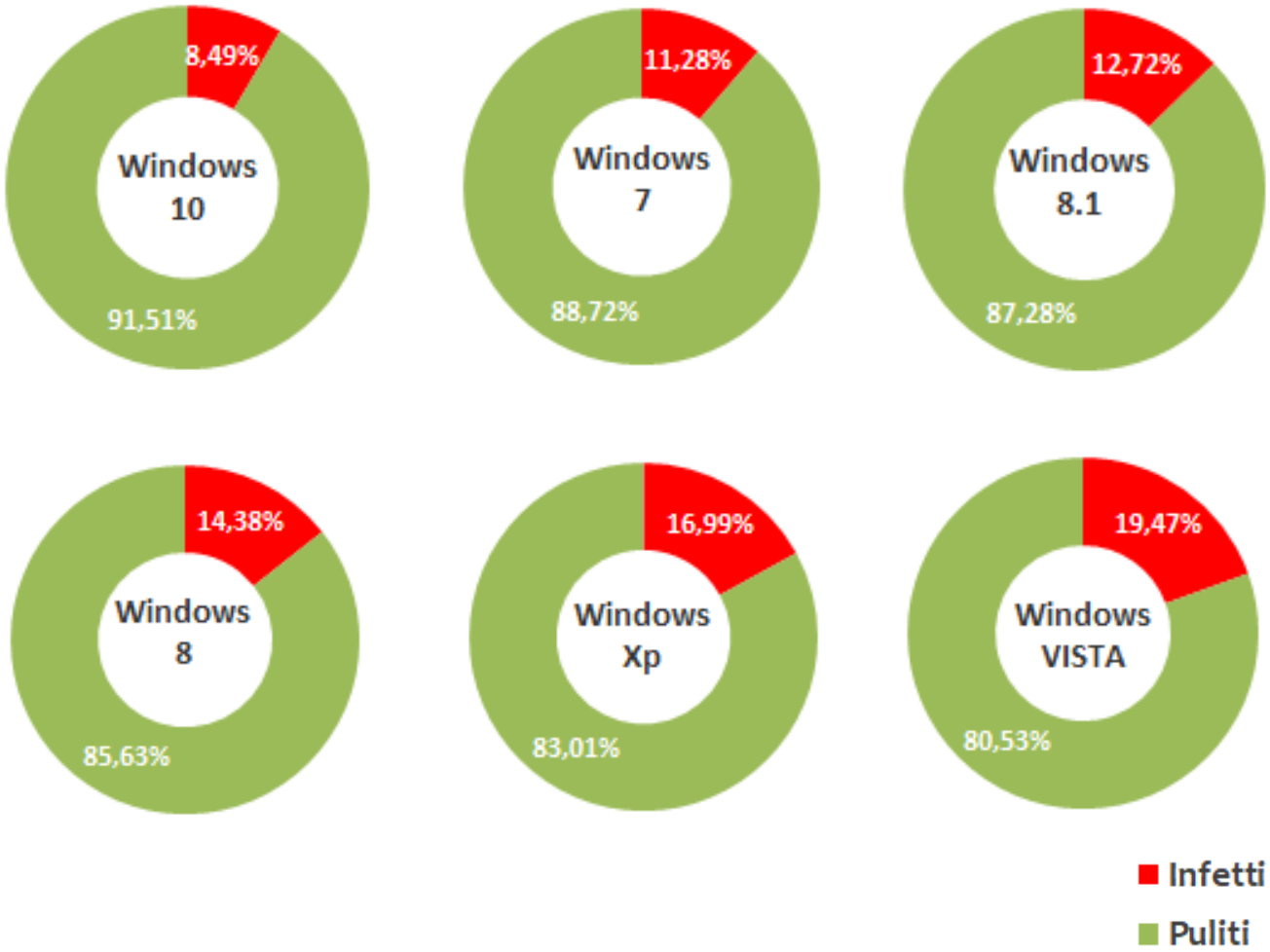
- 65,66% client con Windows 10
- 26,28% client con Windows 7
- 8,06% client con altri s.o. Windows



Windows 10 e **Windows 7** coprono poco meno del 92% 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 9,10% ancora lievemente in crescita rispetto a dicembre che era del 8,49%. 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.

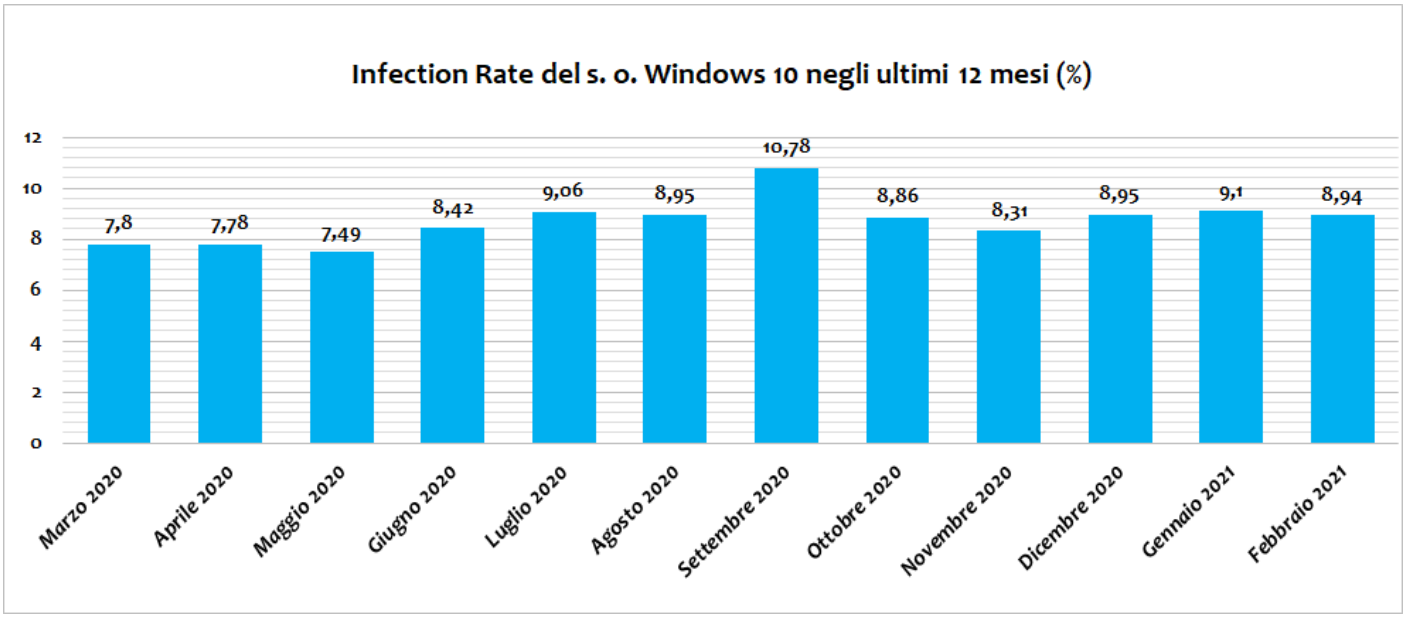
Paragonando I due più vecchi sistemi con Windows 10, si può notare infatti che l'IR di entrambi è più del doppio rispetto al più recente prodotto di Microsoft 8,49% vs 16,99%!

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 dicembre 2019 fino a metà febbraio 2020, per poi riprendere la sua attività dal mese di luglio 2020.

La messa fuori gioco di Emotet a Gennaio 2021 potrebbe essere una delle cause che ha riportato il rate di infezione di Windows 10 sotto la soglia dei nove punti percentuali (8,94%).

Nel Cyber-Threat Report 2021-01 alla sezione EMOTET è possibile consultare interessanti informazioni sulla vicenda.



TG Soft
Cyber Security Specialist
www.tgsoft.it