Cyber-Threat Report

Novembre 2020

TG Soft
Cyber Security Specialist
www.tgsoft.it

Novembre 2020

TG Soft
Cyber-Threat Report

Notizie di rilievo:

Vulnerabilità VPN con attacco ransomware

Panorama delle minacce in Italia a novembre

Sommario:

Nel mese di novembre si è riscontrato una leggera flessione degli attacchi informatici ed un leggero calo del numero dei cluster di malware rispetto al mese di ottobre.

Emotet è stato il grande assente di questo mese. Le sue campagne di malspam sono cessate il 31 ottobre e nel mese di novembre si è limitato ad aggiornare il proprio modulo.

L'assenza di Emotet ha portato alla ribalta **AgentTesla, Ursnif** e **LokiBot.**

AgentTesla e **LokiBot** sono dei password stealer utilizzati da diversi cyber-attori in Italia.

Ursnif è stato molto attivo con numerose campagne nel mese di novembre. Altri password stealer e RAT si sono fatti notare in questo mese e sono: **Ave_Maria; FormBook** e **AdWind.** In questo mese abbiamo registrato un aumento degli attacchi ransomware, molti dei quali veicolati via RDP o VPN, tra questi possiamo annoverare **VoidCrypt, Dharma, Phobos, Matrix** e **LockBit.**

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.

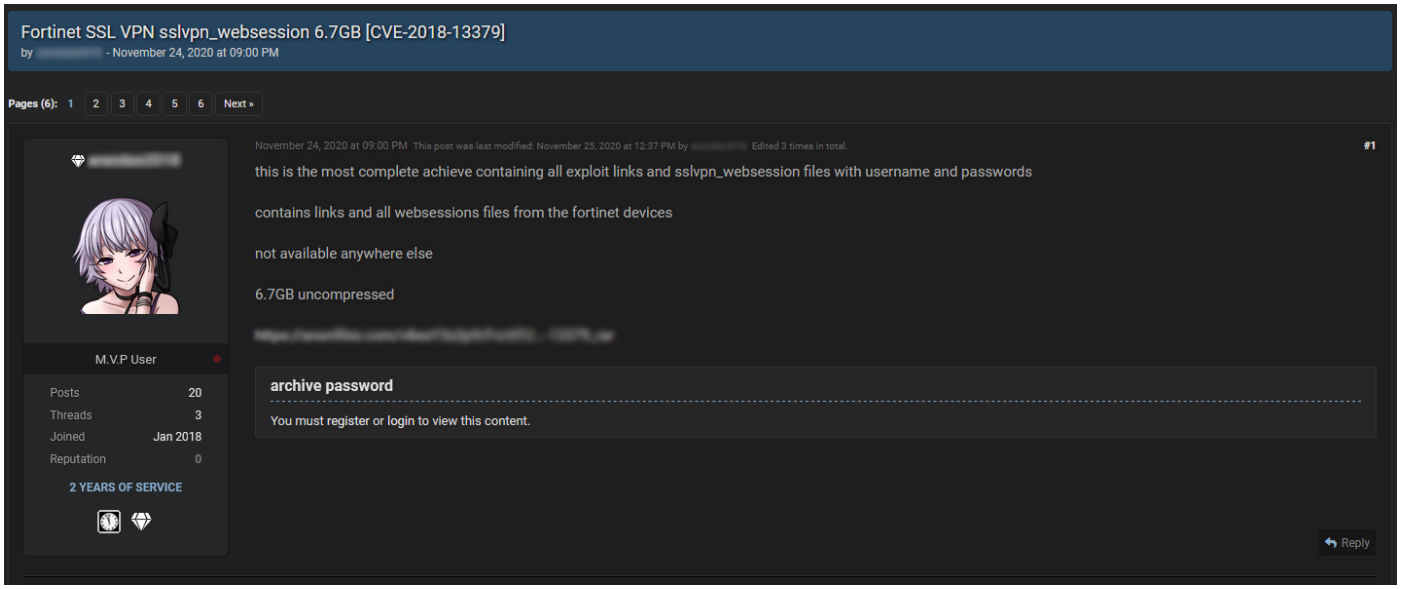
"Infection Rate: è la percentuale degli utenti che hanno incontrato almeno una minaccia segnalata al C.R.A.M. di TG Soft"

Vulnerabilità VPN con attacco ransomware

Website Antivirus Illustration by WOOBRO DESIGN

Nel mese di Novembre vari cyber-criminali hanno pubblicato nei forum del DarkWeb varie liste di IP gestiti dal firewall Fortinet vulnerabili all'exploit CVE-2018-13379.

Vediamo in seguito uno dei vari post disponibili nel DarkWeb:



Le varie liste comprendono oltre 50000 IP ancora vulnerabili sparsi in tutto il globo, appartenenti sia a piccole aziende che a grandi enti pubblici, istituti bancari e grandi aziende.

L'exploit CVE-2018-13379, datato 2018 permette grazie ad una semplice chiamata WEB non autenticata all'interfaccia di gestione del dispositivo di ottenere le credenziali degli accessi VPN (utente/password). Attraverso la connessione VPN è possibile accedere in remoto alla rete interna aziendale (LAN) dando potenziale accesso a tutti i dispositivi (PC/SERVER/NAS ecc.) presenti in rete.

L'NVD ha classificato la vulnerabilità come 9.8 su 10 (CRITICAL).

Le versioni del firmaware affette dalla vulnerabilità sono:

- FortiOS 6.0: 6.0.0 to 6.0.4
- FortiOS 5.6: 5.6.3 to 5.6.7
- FortiOS 5.4: 5.4.6 to 5.4.12

Il vendor ha provveduto a rilasciare gli aggiornamenti necessari a correggere la vulnerabilità (FortiOS 5.4.13, 5.6.8, 6.0.5 o 6.2.0 e successivi) ma nonostante sia passato oltre un anno dal rilascio della patch, molti dispositivi sono rimasti vulnerabili.

I cyber-criminali stanno sfruttando l'occasione per penetrare le reti locali protette dal sistema VPN vulnerabile eseguendo attacchi ransomware e/o esfiltrando dati riservati.

Il caso REALE analizzato dal C.R.A.M. di TG Soft

Il C.R.A.M. di TG Soft in data 05 novembre ha analizzato un attacco ransomware perpetrato sfruttando la vulnerabilità CVE-2018-13379.

Vediamo in primis la cronistoria degli eventi:

1. 05/11 ore 03:33 primo accesso via VPN vulnerabile alla rete LAN da un IP localizzato in Turchia
2. 05/11 ore 06:52 circa effettuato accesso RDP ad un primo server utilizzato come TERMINAL SERVER dove il cyber-criminale ha utilizzato vari Tools.
3. 05/11 ore 07:26 circa effettuato accesso via RDP ad un secondo server utilizzato come BACKUP SERVER
4. 05/11 ore 07:35 circa eseguito il ransomware VoidCrypt sul BACKUP SERVER

Il ransomware utilizzato per tentare di cifrare i dati appartiene alla famiglia del VoidCrypt e una volta cifrati i dati avranno la seguente struttura:

[NOME_FILE_ORIGINALE].[ESTENSIONE_FILE_ORIGINALE].**[lilmoon7766@criptext.com]**
[ID_CLIENTE_15_CIFRE_ALFANUMERICHE].**Spade**

Viene inoltre lasciato il file con le istruzioni del riscatto: Read-For-Decrypt.HTA che vediamo di seguito:

Il cyber-criminale si è servito inoltre di vari Tools per l'analisi della rete locale LAN e per eseguire varie attività come:

- Advanced_Port_Scanner
- Unlocker.1.9.2.Portable
- ransom.cmd
- good.txt

Il file ransom.cmd è un batch utilizzato per cancellare le shadow copy dal PC/SERVER, per disabilitare il firewall locale e per eseguire delle modifiche sulle configurazioni di startup del Sistema Operativo, vediamo di seguito le istruzioni utilizzate nel batch:

```
vssadmin delete shadows /all /quiet
wmic shadowcopy delete
bcdedit /set {default} bootstatuspolicy ignoreallfailures
bcdedit /set {default} recoveryenabled no
wbadmin delete catalog -quiet
netsh advfirewall set currentprofile state off
netsh firewall set opmode mode=disable
```

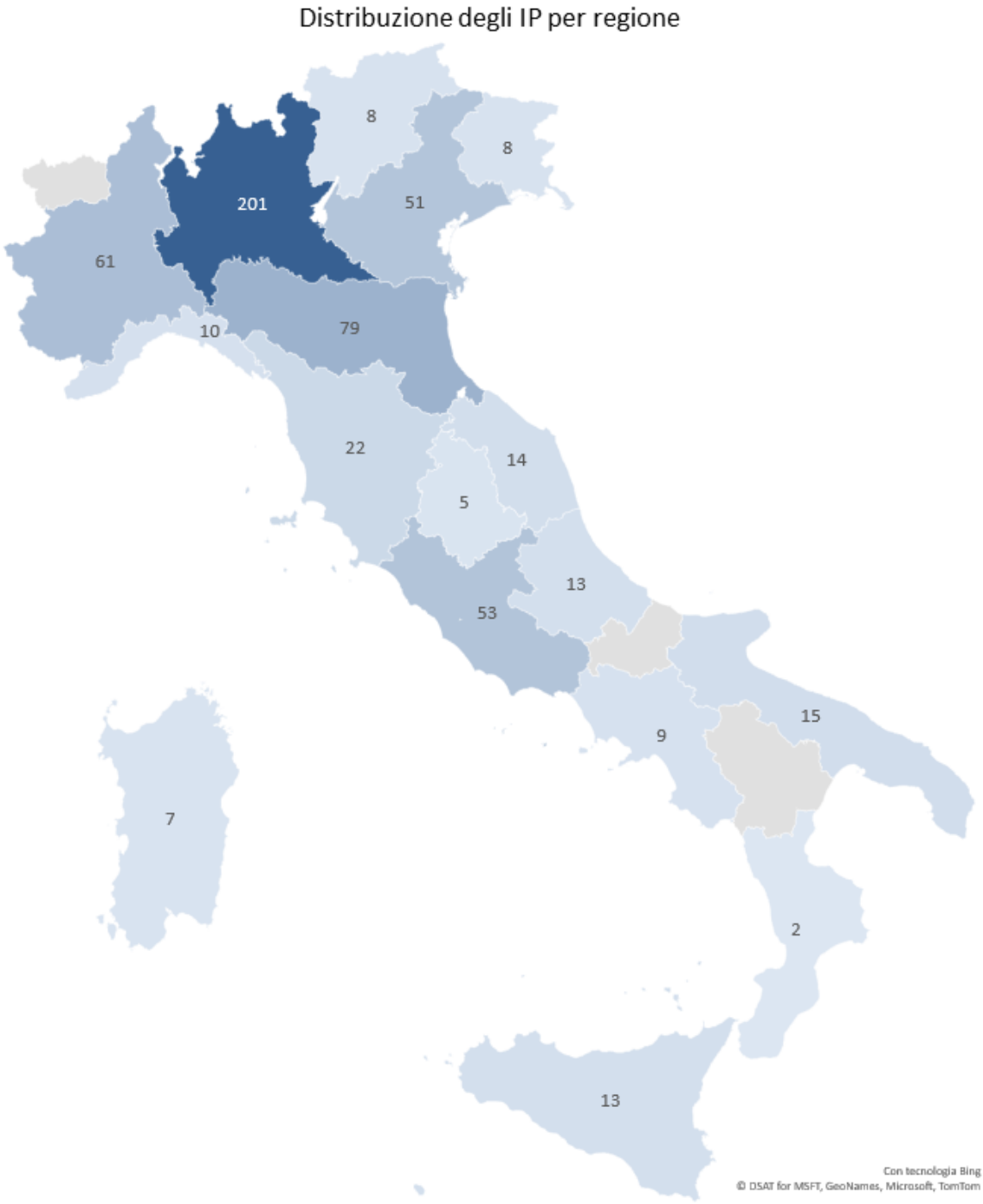
Interessante è il file good.txt lasciato dal cyber-criminale nel primo server, si tratta di una lista di 571 IP con porta 10443.

La porta 10443 è proprio la porta associata al servizio vulnerabile Fortinet SSL VPN.

Di questa lista, 570 IP risultano essere localizzati in Italia. Si tratta quindi molto probabilmente di un primo sotto insieme specifico al target Italiano degli IP vulnerabili pubblicati successivamente nella seconda metà di Novembre nei vari forum del DarkWeb.

Questo dimostra che già ad inizio Novembre i cyber-criminali si sono organizzati per sfruttare questa vulnerabilità per effettuare gli attacchi.

Vedremo di seguito la distribuzione geografica di questi IP con target Italia:

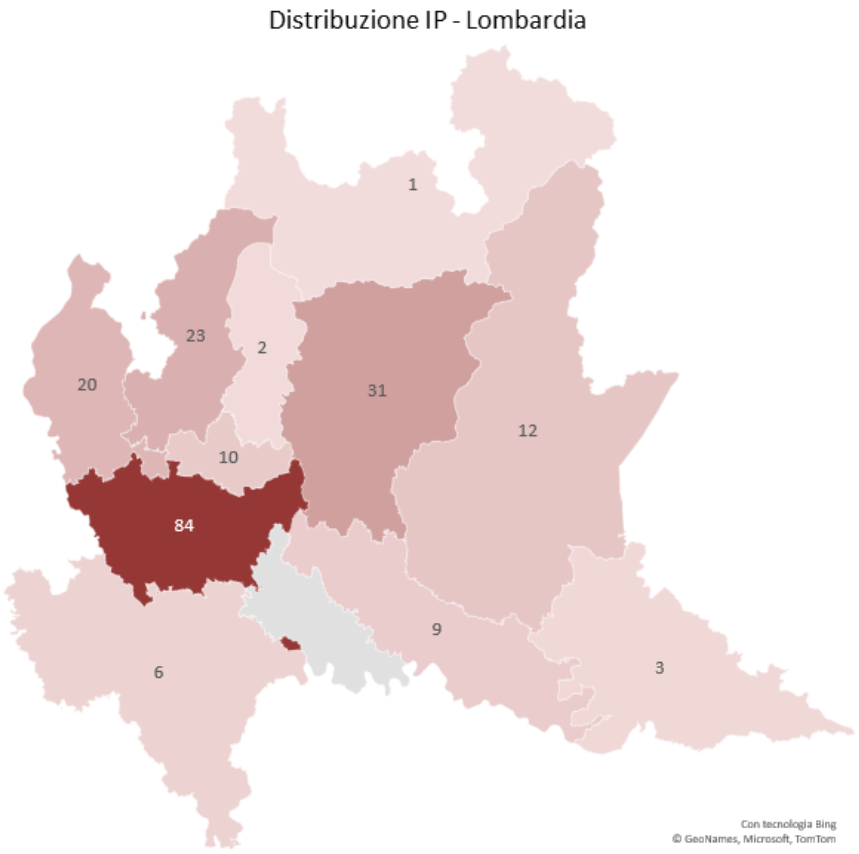


Le regioni più colpite sono:

- Lombardia
- Emilia Romagna
- Piemonte
- Lazio
- Veneto

Nella figura sottostante possiamo vedere la distribuzione degli IP nelle regione Lombardia.

La provincia di Milano è quella che ha il maggior numero di IP vulnerabili alla CVE-2018-13379.

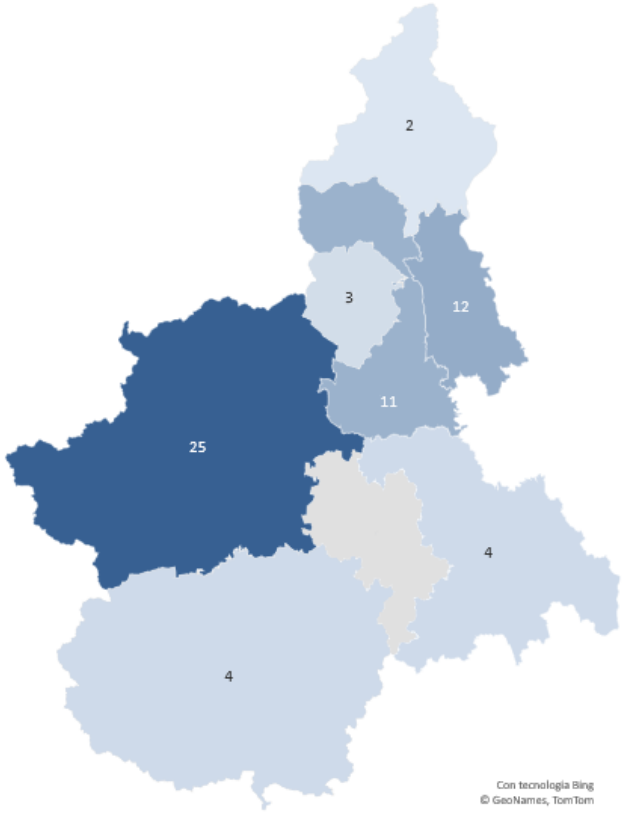


Provincia	Num. IP
Milano	84
Bergamo	31
Como	23
Varese	20
Brescia	12
Monza e Brianza	10
Cremona	9
Pavia	6
Mantova	3
Lecco	2
Sondrio	1

Nella regione dell'Emilia Romagna, la maggior parte degli IP sono geolocalizzati nelle province di Bologna, Modena e Reggio Emilia. Invece nella regione Lazio gli IP sono geolocalizzati tutti nella provincia di Roma.

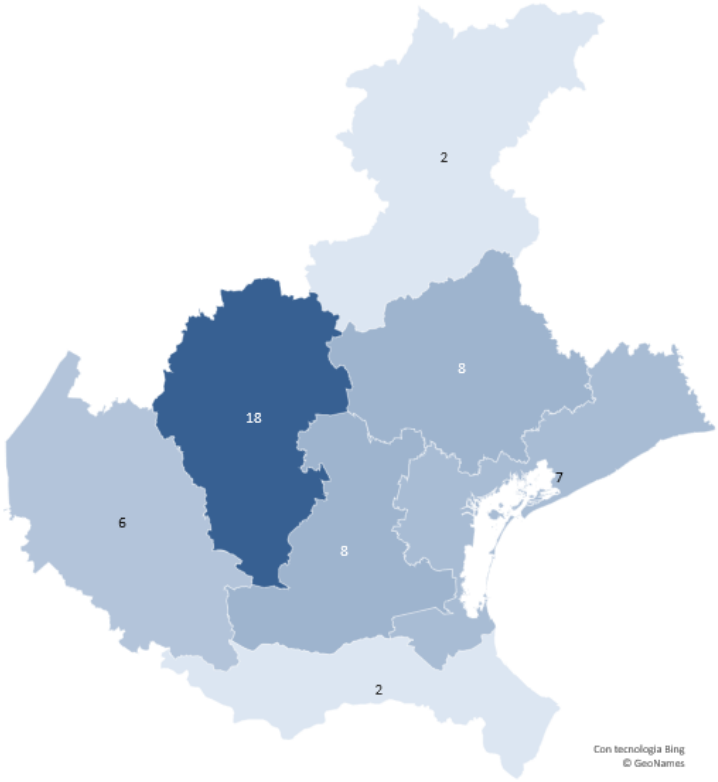
Nelle figure sottostanti possiamo vedere la distribuzione degli IP nelle regioni Piemonte e Veneto.

Distribuzione IP - Piemonte



Provincia	Num. IP
Torino	25
Novara	12
Vercelli	11
Alessandria	4
Cuneo	4
Biella	3
Verbano-Cusio-Ossola	2

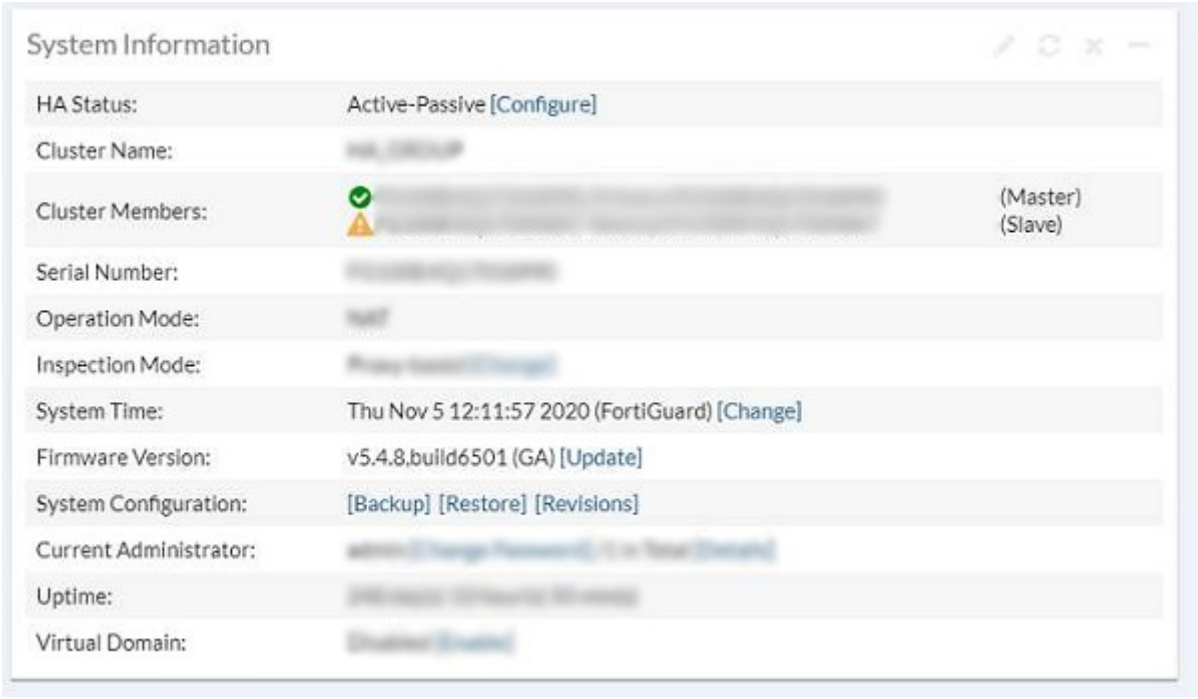
Distribuzione IP - Veneto



Provincia	Num. IP
Vicenza	18
Padova	8
Treviso	8
Venezia	7
Verona	6
Belluno	2
Rovigo	2

In seguito si è proceduto a verificare i log di sicurezza dei due server da cui si è riscontrato che il primo accesso al TERMINAL SERVER è avvenuto attraverso il sistema VPN. Si è perciò proceduto ad analizzare i LOG di accesso del firewall avendo quindi la conferma dell'avvenuto accesso via VPN dal'IP localizzato in Turchia.

L'accesso via VPN è stato eseguito sfruttando la vulnerabilità CVE-2018-13379 infatti il firewall a seguito di verifica è risultato vulnerabile, conferma ottenuta anche grazie alla verifica della versione del firmware (v 5.4.8) installata nel dispositivo:

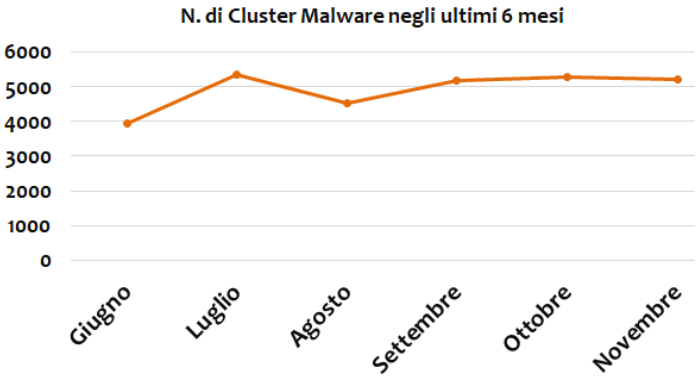


Non è superfluo ricordare che una delle best-practice fondamentali per un buon mantenimento del livello di sicurezza è proprio quella di eseguire regolarmente gli aggiornamenti software/firmware di tutti gli apparati collegati in rete e dove possibile di attivare gli aggiornamenti automatici.

Statistiche Malware

Novembre 2020—ITALIA

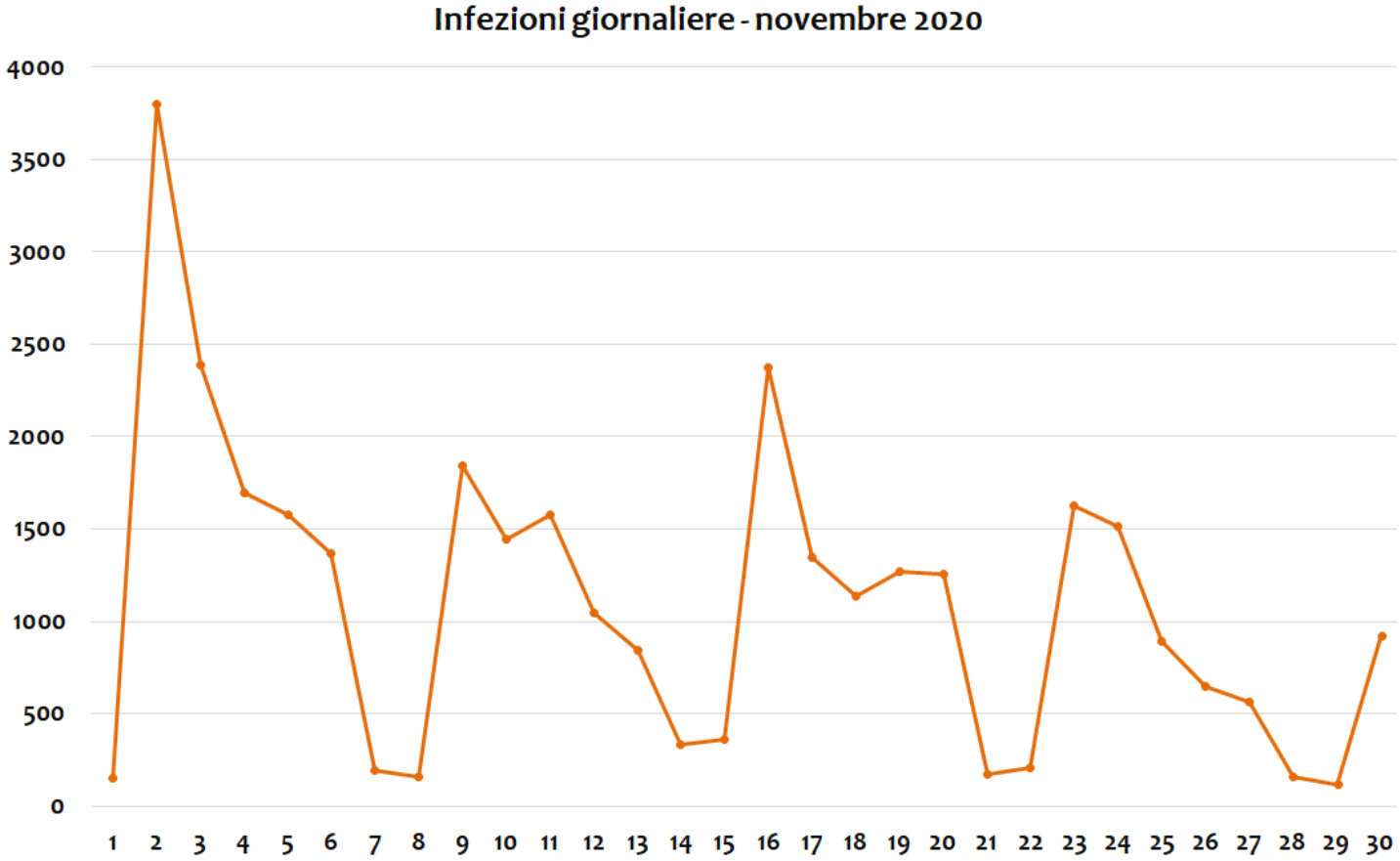
I dati della telemetria del C.R.A.M. di TG Soft sono raccolti dagli utenti che utilizzano il software anti-virus Vir.IT eXplorer. Le segnalazioni derivano da attacchi bloccati oppure malware riscontrati all'interno del parco macchine monitorato. Ogni minaccia identificata da Vir.IT viene classificata 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 novembre abbiamo avuto una leggera flessione del numero di malware rispetto al precedente mese di ottobre, dove erano stati riscontrati 5280 cluster di malware contro i 5227 del mese di novembre (-1,0%).

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

All'inizio del mese abbiamo avuto un picco di segnalazioni d'infezione, dovute alle scansioni automatiche mensili del motore anti-virus Vir.IT eXplorer. Nelle settimane successive, abbiamo un incremento delle segnalazioni il lunedì, per poi calare in modo progressivo nei giorni successivi. L'andamento delle infezioni a novembre è stato abbastanza uniforme, non vi sono stati attacchi massivi come era successo nei mesi scorsi, poiché Emotet ha deciso di prendersi un periodo di pausa.



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

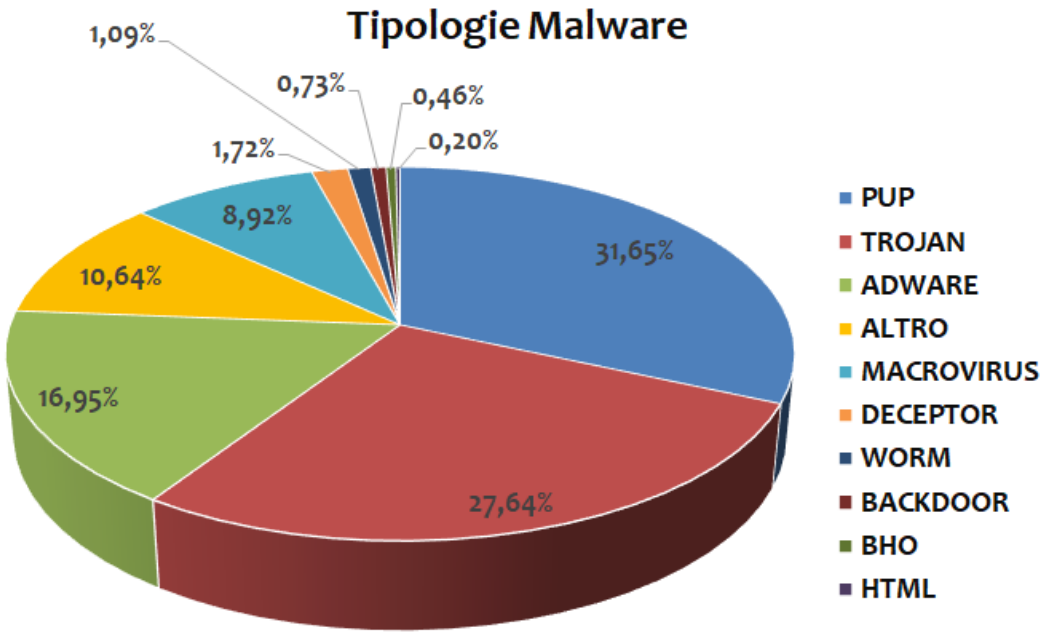
I malware si suddividono in diverse tipologie: Adware, Backdoor, Trojan, Worm, Virus, PUA/PUP, Deceptor, etc.

Nel mese di novembre la tipologia dei **PUP** si riconferma in prima posizione con il 31,65% delle infezioni, relegando la famiglia dei **TROJAN** al secondo posto con il 27,64%. Al terzo posto troviamo gli **ADWARE** con il 16,95% in crescita rispetto a ottobre. Al quarto posto troviamo il gruppo denominato **ALTRO**, che include i virus, con il 10,64% delle infezioni in leggero calo rispetto al mese scorso. I **MACROVIRUS** perdono un'altra posizione a novembre e si piazzano al quinto posto. Questo calo dei MACROVIRUS è dovuto alla pausa che si è preso Emotet, che ha portato ad un drastico calo d'infezioni.

E' interessante notare che le prime 4 tipologie di malware rappresentano quasi l'87% delle infezioni monitorate.

In sesta posizione troviamo anche questo mese i **DECEPTOR** con l'1,72%, seguono **WORM** con lo 1,09% e chiudono la classifica: **BACKDOOR; BHO** e **HTML.**

I PUP si riconfermano in prima posizione, brusco calo della famiglia dei MACROVIRUS, dovuto alla pausa che si è preso Emotet.



Analizziamo le statistiche di novembre dei singoli Malware. Questo mese si riconferma al primo posto il **PUP.Win32.MindSpark.F** con il 6,19% delle infezioni, che può compromettere il tuo browser, modificando l'home page e il motore di ricerca.

Al secondo posto troviamo **Office.VBA_Macro_Heur** (tipologia MACRO VIRUS) con l'1,82% delle infezioni, in decremento di quasi 4 punti percentuali rispetto al mese scorso.

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

Al terzo posto troviamo il **PUP.Win32.CheatEngine** con l'1,78% delle infezioni rilevate. In quarta posizione troviamo un altro PUP della famiglia **CheatEngine** con l'1,78% delle infezioni.

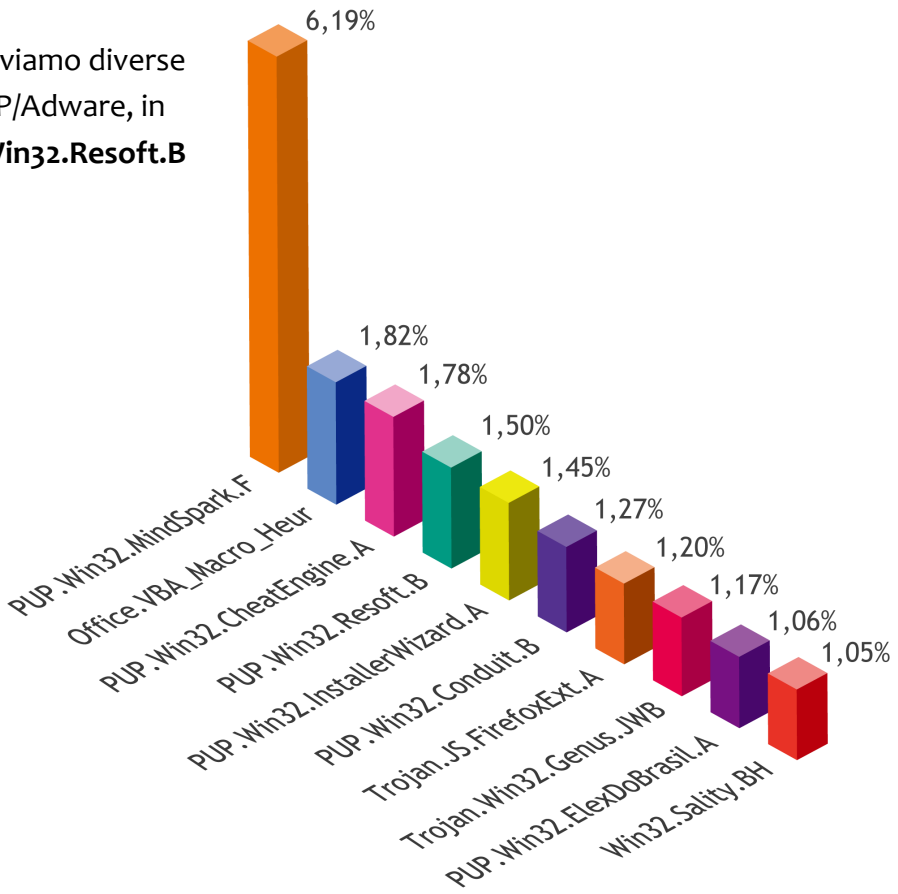
Anche questo mese nella Top10 troviamo diverse vecchie conoscenze del mondo PUP/Adware, in quarta posizione troviamo il **PUP.Win32.Resoft.B** e il **PUP.Win32.Counduit.B** in sesta.

I malware della Top10 rappresentano il 18,49% delle infezioni di novembre, il rimanente 81,52% è dato da altri 5217 cluster di malware.

Chiude in decima posizione il virus **Win32.Sality.BH**.

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

I malware della Top10 rappresentano il 18,49% delle infezioni del mese di novembre, il rimanente **81,52%** è dato da altri 5217 cluster di malware.

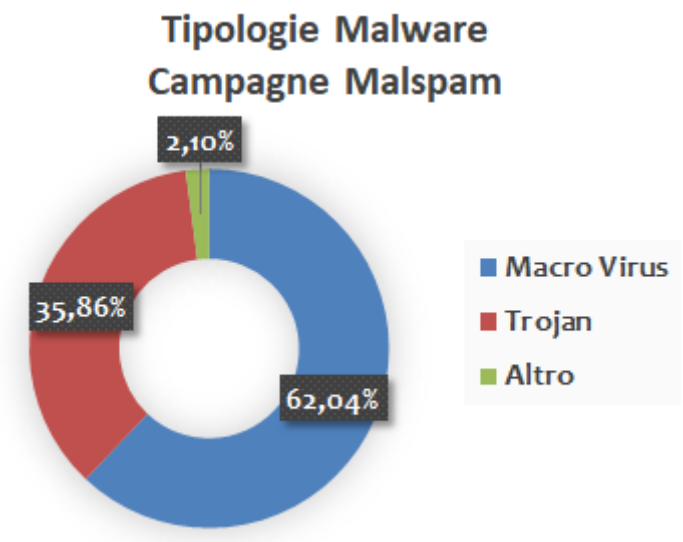


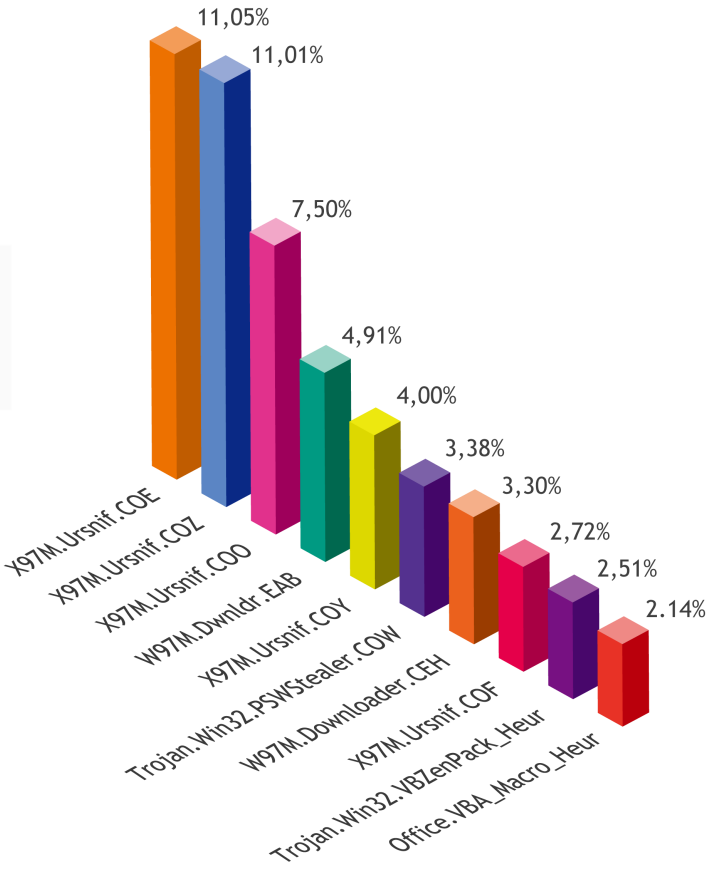
Statistiche Malware via email

Novembre 2020 - ITALIA

Analizziamo ora le campagne di malware veicolate via email nel mese di novembre. 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 62,04% (-13,27%). Il dato ottenuto, segna un calo rispetto al mese scorso, grazie alla pausa che si è preso Emotet. Seguono la tipologia dei **TROJAN** che con il 35,86% (+12,0%) si confermano al secondo posto. Al terzo posto troviamo la tipologia **ALTRO** con il 2,10% che include varie tipologie come **WORM** e **BACKDOOR**.





Analizzando le statistiche delle campagne di malspam per singolo malware, al primo posto troviamo il trojan bancario chiamato **Ursnif** con la variante **.COE** con l'11,05%. Ursnif a novembre è salito alla ribalta conquistando tutto il podio ed inoltre, lo troviamo in 5ª e in 8ª posizione, piazzando così ben 5 varianti nella Top10.

In quarta e in settima posizione troviamo due varianti di **W97M.Dwnldr,** rispettivamente le varianti **.EAB** e **.CEH**. In sesta e in nona posizione troviamo il **Trojan.Win32.PSWStealer.COW** e il Trojan.Win32.VBZenPack_Heur. Chiude in decima posizione l'**Office.VBA_Macro_EUR** (tipologia Macro Virus) , che include l'intercettazione generica di diverse famiglie di macro virus.

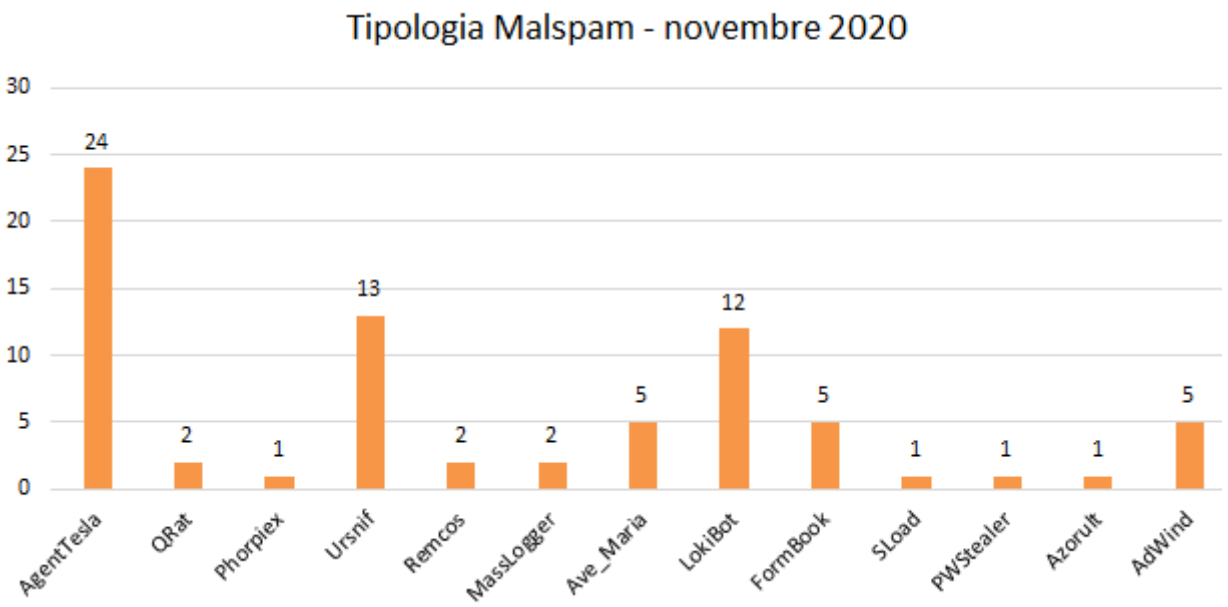
Nella Top10 delle mail, troviamo quasi esclusivamente MACRO VIRUS, che rappresentano il 46,63% delle infezioni di novembre, il rimanente 53,37% è dato da altri 174 malware.

A novembre il grande assente a livello mondiale è stato Emotet.

Analisi dei malware di novembre

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

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



A novembre balza all'occhio l'assenza del malware **Emotet,** che si è preso una pausa a partire dal 31 ottobre. La botnet di Emotet continua ad essere ancora attiva, ma non sta inviando campagne di malspam.

Questo mese il primo posto è aggiudicato da **AgentTesla,** un password stealer che ruba le credenziali di accesso, risulta essere molto utilizzato da diversi attori cyber-criminali nel mese di novembre.

Il trojan banker **Ursnif** è risultato molto attivo con ben 13 campagne a novembre. Lo scopo di questo malware è di rubare le credenziali di accesso all'home banking per svuotare il conto corrente.

LokiBot continua ad essere molto utilizzato e lo troviamo con ben 12 campagne.

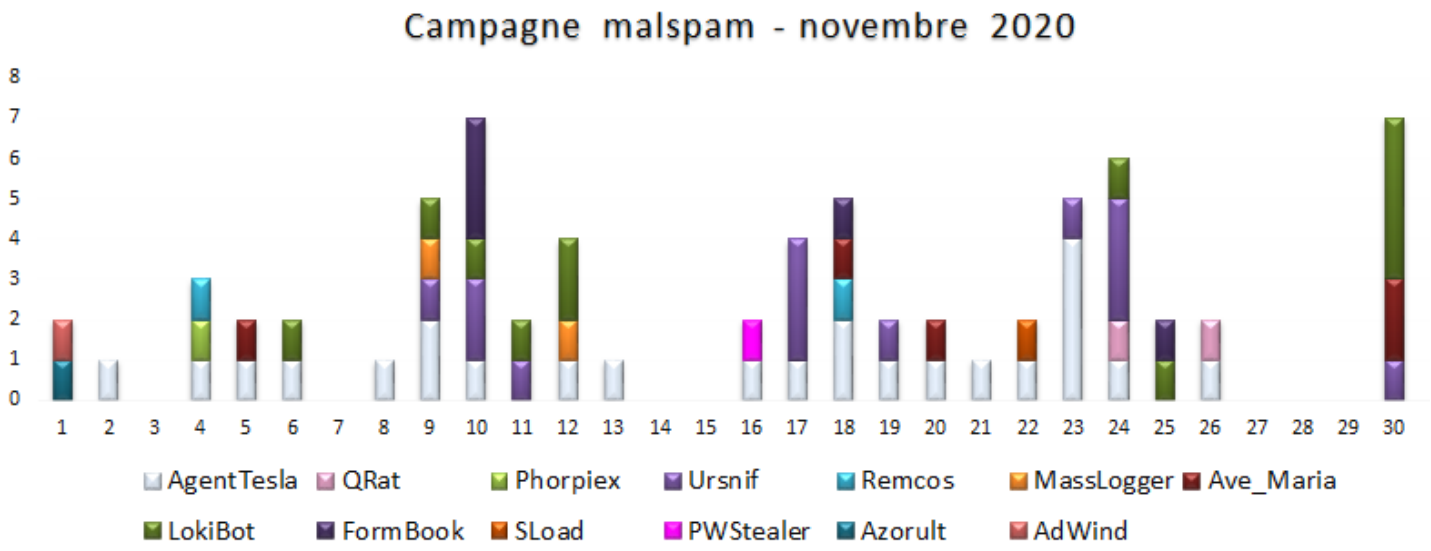
Sono continuate le campagne di diversi RAT come **AdWind, Ave_Maria** e **FormBook**.

A novembre è ritornato il malware **Phorpiex**, ma questa volta non ha distribuito il ransomware **Avaddon**.

Altro assente con campagne dirette all'utenza italiana è il cyber-attore **Hagga,** che però ha continuato con campagne malspam internazionali.

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

Nel mese di novembre abbiamo monitorato quasi ogni giorno campagne di malspam di AgentTesla, a dimostrare che questo password stealer è utilizzato da diversi cyber-criminali che hanno nel mirino l'utenza italiana. Ogni settimana di novembre possiamo trovare campagne di Ursnif e LokiBot, la cui veicolazione durante il mese è avvenuta in modo uniforme. A novembre abbiamo registrato due picchi di campagne indirizzate all'utenza italiana, che sono avvenute rispettivamente martedì 10 e lunedì 30 novembre, dove sono state diffuse 7 campagne di malspam, che hanno veicolato rispettivamente 4 e 3 differenti famiglie di malware.



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

Week 44 ==> dal 31 ottobre al 6 novembre

Week 45 ==> dal 7 al 13 novembre

Week 46 ==> dal 14 al 20 novembre

Week 47 ==> dal 21 al 27 novembre

Week 48 ==> dal 28 novembre al 4 dicembre

Ursnif

Analisi delle campagne di novembre

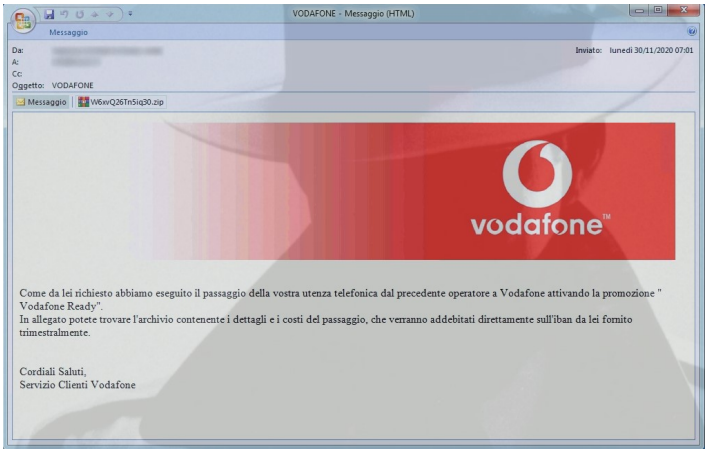
Analizziamo ora le campagne del malware bancario **Ursnif** (noto anche come **Gozi** o **IFSB**) nel mese di novembre.

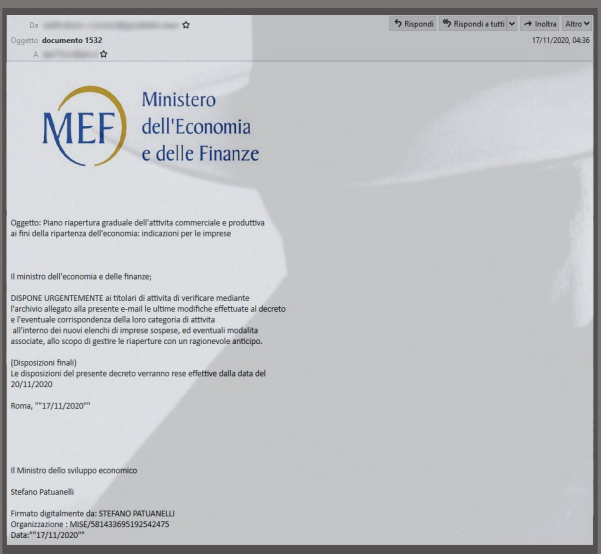
Come abbiamo visto, questo malware è uno dei più diffusi via email in Italia, a novembre è stato veicolato attraverso 13 campagne di malspam.

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

Le campagne veicolate da Ursnif hanno avuto i seguenti temi:

- Ministero dello Sviluppo Economico (3)
- INPS (2)
- Enel Energia (2)
- B.R.T. S.p.A. (3)
- Agenzia delle Entrate (2)
- Vodafone (1)



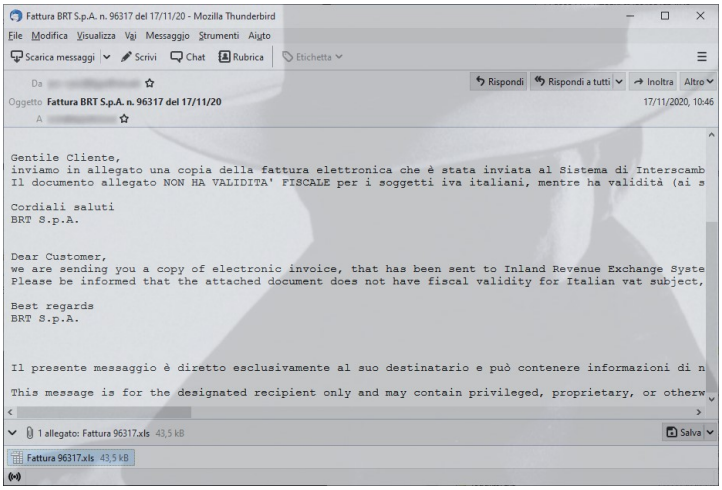


Ursnif—Campagne Malspam

09/11/2020	Ministero dello sviluppo Economico
10/11/2020	INPS
10/11/2020	Enel Energia
11/11/2020	INPS
17/11/2020	Ministero dello sviluppo Economico
17/11/2020	Fattura B.R.T. S.p.A.
17/11/2020	Rimessa B.R.T. S.p.A.
19/11/2020	Ministero dello sviluppo Economico
23/11/2020	Agenzia delle Entrate
24/11/2020	Agenzia delle Entrate
24/11/2020	Fattura B.R.T. S.p.A.
24/11/2020	Enel Energia
30/11/2020	Vodafone

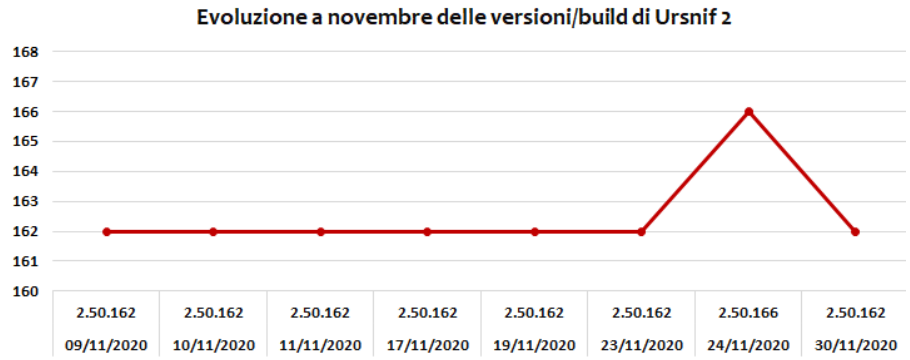
Dall'analisi delle campagne di malspam e dalle configurazioni individuate all'interno del trojan bancario Ursnif utilizzato, vi sono due gruppi distinti che stanno sfruttando questo malware a novembre per attaccare l'utenza italiana. Il primo gruppo ha veicolato ben 8 campagne di malspam a tema MEF, INPS, Agenzia delle Entrate e Vodafone, invece il secondo si è limitato a cinque campagne a tema "B.R.T. S.p.A." e " Enel Energia".

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



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

- Versione 2;
- Versione 3.

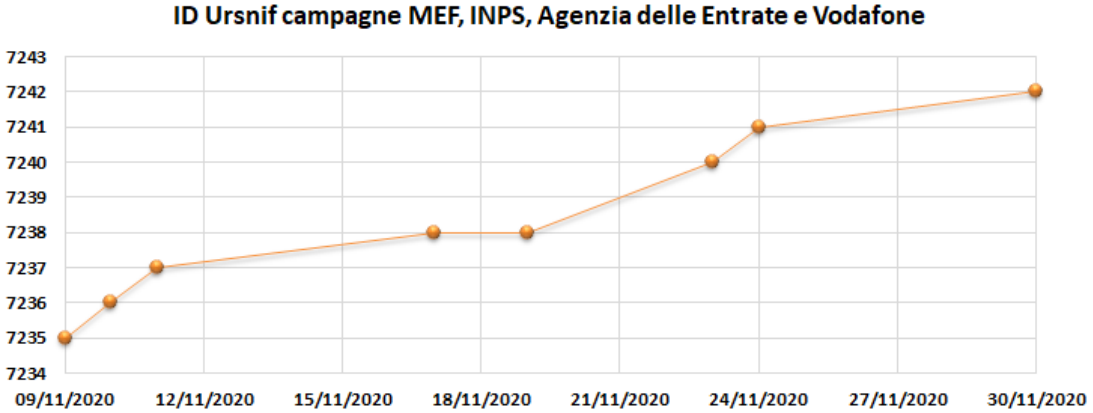


In Italia sono circolate, fino ad aprile, entrambe le versioni, ma nel mese di novembre è stata rilevata esclusivamente la versione 2.

Nel mese di novembre sono stati rilasciati due aggiornamenti del malware Ursnif, il 9 novembre siamo passati dalla build 2.50.161 alla 2.50.162 e il 24 novembre è stata rilasciata la build 2.50.166.

La build 2.50.166 è stata utilizzata solamente dal gruppo che utilizza nelle campagne il tema "BRT S.p.a.", invece l'altro gruppo nella campagna del 20 novembre di "Vodafone" ha continuato ad utilizzare la build 162.

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



Ransomware

Novembre 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:

- **Avaddon;**
- **VoidCrypt;**
- **Dharma;**
- **Stop/Djvu;**
- **MAOLOA;**
- **Phobos;**
- **LockBit;**
- **Matrix.**

I ransomware identificati a novembre derivano da attacchi attraverso il desktop remoto (RDP) mirati verso aziende italiane, vulnerabilità di VPN, scaricati da altri malware oppure dal download di software infetto.

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 cybercriminale o attaccante cerca di disinstallare l'antivirus o di renderlo inefficace, in modo che l'attacco ransomware abbia successo.

L'attacco ransomware **Avaddon** è avvenuto attraverso uno script di POWERSHELL che conteneva il payload del malware. L'infezione potrebbe essere scaturita dalla navigazione su siti compromessi.

VoidCrypt è stato utilizzato nell'attacco avvenuto sfruttando la vulnerabilità della VPN del firewall FortiGate di Fortinet, la quale ha permesso di accedere alla rete locale e quindi di conseguenza ai server tramite RDP.

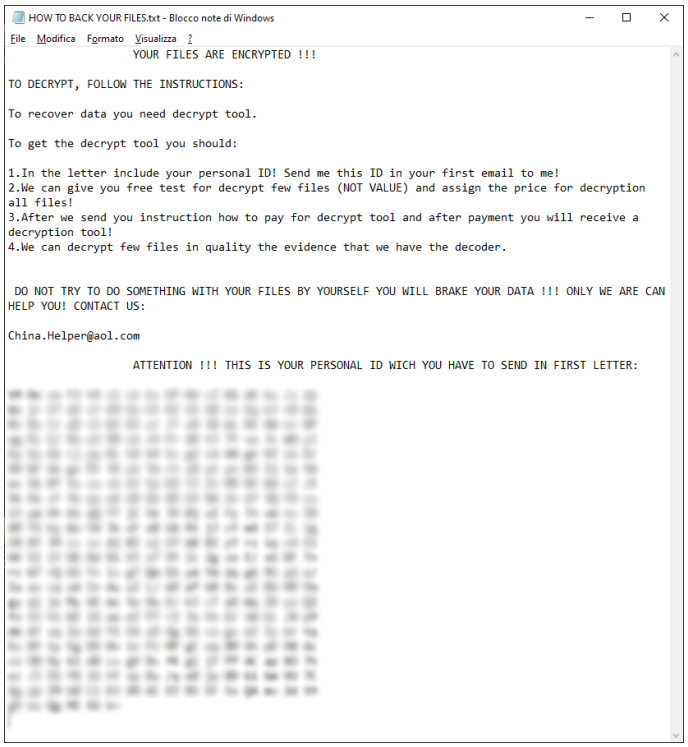
Nella figura sotto possiamo vedere la richiesta di riscatto di **VoidCrypt**.

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

- .259
- .ROGER

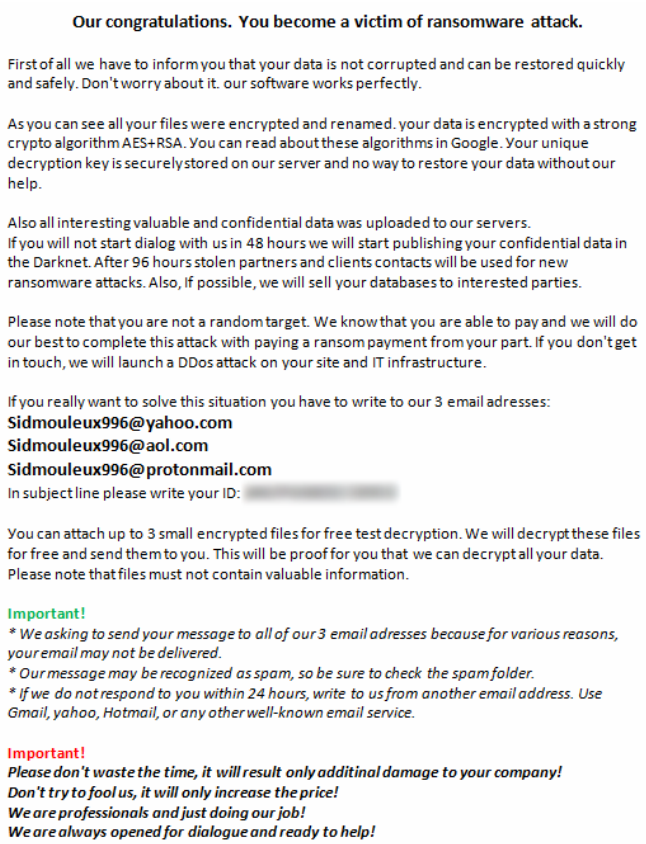
Sotto vediamo le istruzioni di riscatto del ransomware **Phobos**.

Il ransomware **MAOLOA** è stato scaricato attraverso il malware **QakBot** con cui il pc era precedentemente infetto. Nella figura a destra possiamo vedere le istruzioni di riscatto.



Anche il ransomware **Matrix** è stato veicolato attraverso un attacco RDP.

Nella figura sotto possiamo vedere le istruzioni di riscatto richieste dal ransomware Matrix.



Our congratulations. You become a victim of ransomware attack.

First of all we have to inform you that your data is not corrupted and can be restored quickly and safely. Don't worry about it. our software works perfectly.

As you can see all your files were encrypted and renamed. your data is encrypted with a strong crypto algorithm AES+RSA. You can read about these algorithms in Google. Your unique decryption key is securely stored on our server and no way to restore your data without our help.

Also all interesting valuable and confidential data was uploaded to our servers.
If you will not start dialog with us in 48 hours we will start publishing your confidential data in the Darknet. After 96 hours stolen partners and clients contacts will be used for new ransomware attacks. Also, If possible, we will sell your databases to interested parties.

Please note that you are not a random target. We know that you are able to pay and we will do our best to complete this attack with paying a ransom payment from your part. If you don't get in touch, we will launch a DDos attack on your site and IT infrastructure.

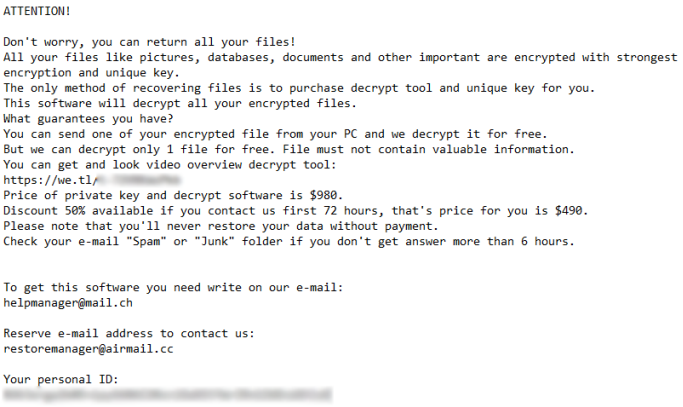
If you really want to solve this situation you have to write to our 3 email adresses:
Sidmouleux996@yahoo.com
Sidmouleux996@aol.com
Sidmouleux996@protonmail.com
In subject line please write your ID:

You can attach up to 3 small encrypted files for free test decryption. We will decrypt these files for free and send them to you. This will be proof for you that we can decrypt all your data.
Please note that files must not contain valuable information.

Important!
** We asking to send your message to all of our 3 email adresses because for various reasons, your email may not be delivered.*
** Our message may be recognized as spam, so be sure to check the spam folder.*
** If we do not respond to you within 24 hours, write to us from another email address. Use Gmail, yahoo, Hotmail, or any other well-known email service.*

Important!
Please don't waste the time, it will result only additinal damage to your company!
Don't try to fool us, it will only increase the price!
We are professionals and just doing our job!
We are always opened for dialogue and ready to help!

Il ransomware **Stop/Djvu** è stato diffuso attraverso il download di software infetti, nella figura sottostante vediamo la richiesta di riscatto di 490 $.



ATTENTION!

Don't worry, you can return all your files!
All your files like pictures, databases, documents and other important are encrypted with strongest encryption and unique key.
The only method of recovering files is to purchase decrypt tool and unique key for you.
This software will decrypt all your encrypted files.
What guarantees you have?
You can send one of your encrypted file from your PC and we decrypt it for free.
But we can decrypt only 1 file for free. File must not contain valuable information.
You can get and look video overview decrypt tool:
https://we.tl/
Price of private key and decrypt software is $980.
Discount 50% available if you contact us first 72 hours, that's price for you is $490.
Please note that you'll never restore your data without payment.
Check your e-mail "Spam" or "Junk" folder if you don't get answer more than 6 hours.

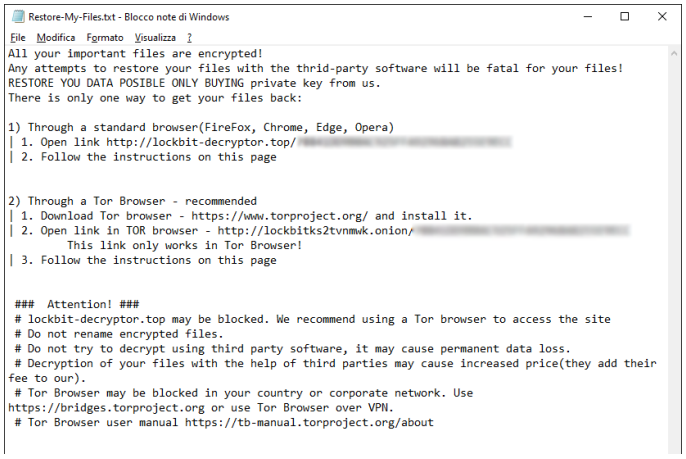
To get this software you need write on our e-mail:
helpmanager@mail.ch

Reserve e-mail address to contact us:
restoremanager@airmail.cc

Your personal ID:

Il ransomware **LockBit** è stato veicolato via RDP contemporaneamente al ransomware **Dharma**. Il cyber-criminale prima ha eseguito **Dharma**, dopo aver visto l'insuccesso del suo attacco, perché bloccato dal sistema anti-ransomware di **Vir.IT**, ha eseguito il **LockBit**.

Nella figura a destra vediamo il riscatto richiesto da **LockBit**.



Il mese di novembre inizia con il comunicato stampa di Maze che annuncia la chiusura ufficiale del progetto ransomware. Nel comunicato viene rinnegata l'esistenza del cartello Maze e indicato il motivo della chiusura del progetto. Nella figura sotto possiamo vedere il comunicato stampa del 1° novembre.

Maze Team official press release. November 1 2020

The Project is closed.

Maze Team Project is announcing it is officially closed.
All the links to out project, using of our brand, our work methods should be considered to be a scam.

We never had partners or official successors. Our specialists do not works with any other software. Nobody and never will be able to host new partners at our news website. The Maze cartel was never exists and is not existing now. It can be found only inside the heads of the journalists who wrote about it.

Attention to everyone who wants for its private information to be deleted from our news website. You can contact to Maze support chat. Support will be continued for a month after the press release.

There were a lot of rumors, lies and speculations around our project. So we decided to answer the questions "why" and "what for".

WHY? Our world is sinking in the recklessness and indifference, in laziness and stupidity. If you are taking the responsibility for other people money and personal data then try to keep it secure. Until you do that there will be more projects like Maze to remind you about secure data storage.

How come that you don't understand that right now a hacker attack is enough for a large area or a country to lose the access to internet, water, gas and electricity. As an instance we had the access to state life support systems of New Yorks and to major internet providers. A good attack was able to cut the access to internet for 35 states. We didn't attack those objects but their security is still disgusting. Think about it. It's not the private case but the security of the whole country and its citizens. One day whose open doors will be passed not by Maze but by some radical psychos whose goals will not just to show you the weakness of security but to make a major damage.

What for? Our world is turning into digital detention camp. Ten or fifteen years and nobody will be able to step aside the system without the fear to lose its social status. Without that social status you won't be able to make purchases or get the social benefits. The first sign was the bitcoin. The digital currency existing only inside the digital world. After some time it will allow its owners to rule the world and to crash the economy of other countries as the gold and currency reserves are not converting into bitcoin. More and more people will work online to be paid with digital currencies. And all the job will be online.

Crypto currencies are going higher and higher and after some time the price will reach a million dollars for a single coin. When all the coins will be dumped by its owners to buy real money. So all the bitcoins will be concentrated by a few people so they will be able to transform the world to a digital platform by ruining it.

With all your recklessness, unawareness and stupidity you are pushing the the world into it. You are slowly turning into a controllable flock. You would not even notice when you will be tagged with chips or your DNA will be the only was to access the new digital world. As it will be the only place you can leave in, to get paid and consume.

All your technologies are a symbol of your helplessness. Once going to wheelchair a man will not be able to walk again. And once trusting your mind to a technology you won't be able to recover your consciousness. By delegation the part of your conscious activity to machines you won't be able to watch at the reality with the clear eye.
You are calling the ones who are killing your mind as your friends and support. And you also calling the ones who are showing you your weakness as the foes and mobsters. The modern world is confusing the cause and the effect, the good and the evil.

Think about it. Try to prevent it. You think that the modern world is a hell. But it's just coming and you are doing much for it.

We will be back to you when the world will be transformed. We will return to show you again the errors and mistakes and to get you out of the Maze.

Ad inizio novembre la società italiana **Campari Group** è stata colpita da un attacco ransomware con esfiltrazione di dati. A darne notizia questa volta è stato il gruppo di cyber-criminali **RAGNAR_LOCKER** attraverso un post nel proprio portale nel dark web.

Security breach of Campari Group network

Ragnar_Locker Team Press Release

We confirm that this attack was made and it was successful. We did encrypt servers of Campari and also downloaded approximately 2TB of sensitive Data from corporate servers.

According Campari's press release from 06/11/2020 they said: "At this stage, we cannot completely exclude that some personal and business data has been taken."

This is ridiculous and looks like a big fat lie, we can confirm that confidential data was stolen and we talking about huge volume of data. So we are suggesting to Campari discard their illusions and if Campari really cares about client's and business confidentiality, they have to contact us to negotiate conditions of the deal and avoid data leakage. We will wait for Campari's response until Tuesday 10th of November 18:00 EST time.

So everyone will see how serious are their intentions about security and confidentiality.

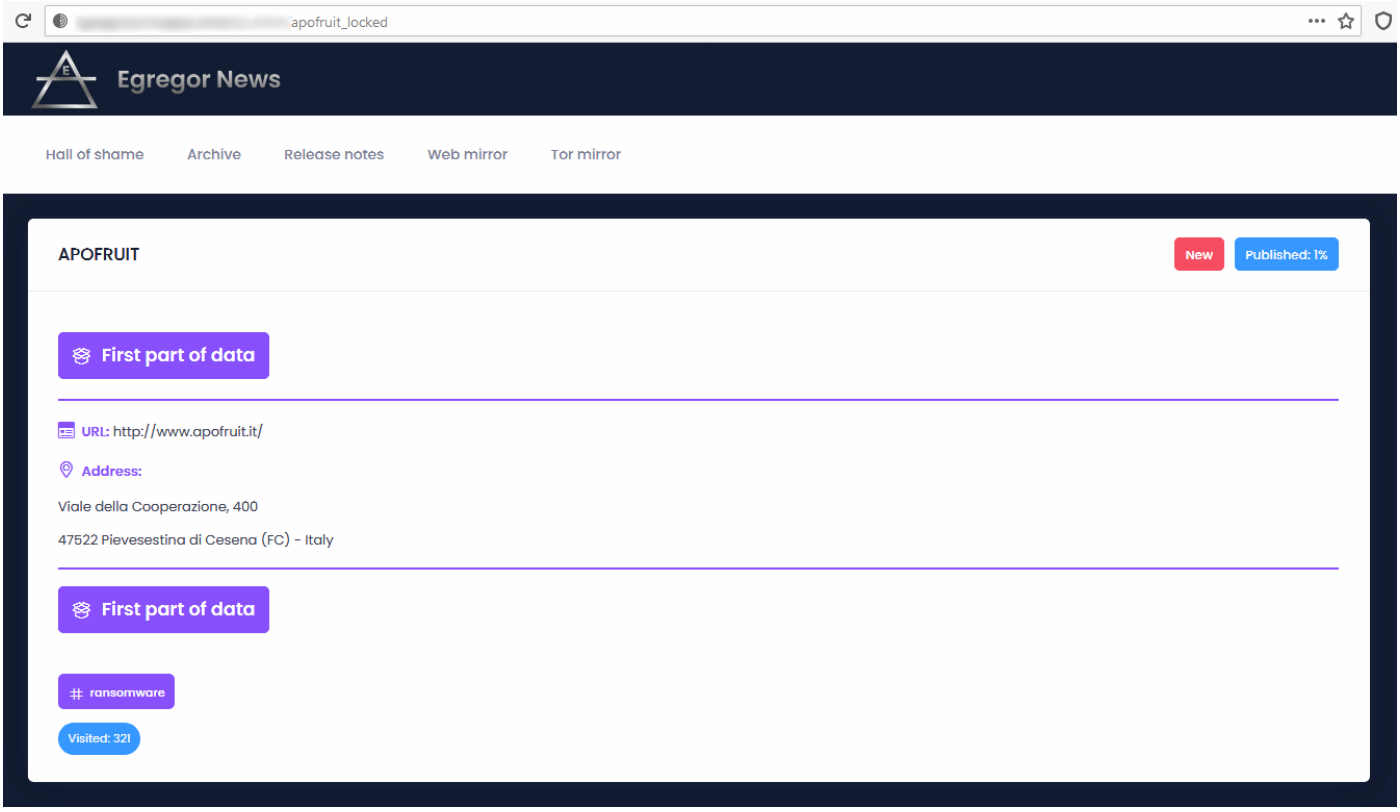
If no deal will be made, all data would be published and\or sold to any third parties.

Il gruppo di cyber-criminali **RAGNAR_LOCKER** ha iniziato a pubblicare i dati esfiltrati come prova dell'attacco a Campari Group.

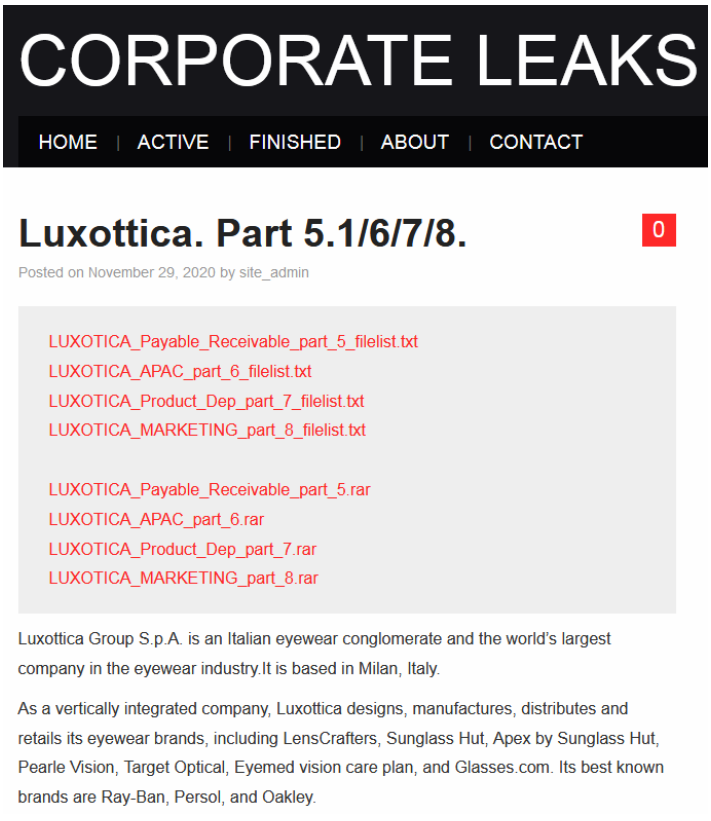
Network Screenshot

Network Screenshot_2

A novembre il gruppo di cyber-criminali di **Egregor** miete un'altra vittima italiana. Questa volta a cadere nel mirino di **Egregor** è la società cesenatica **APOFRUIT**. Nella figura sottostante possiamo vedere la rivendicazione dell'attacco e la pubblicazione di una prima parte di dati esfiltrati.



A fine novembre è stato pubblicato nel dark web l'ultima parte dei dati esfiltrati a **Luxottica** da parte del gruppo cyber-criminale di **Nefilim**.



Prevalenza

Novembre 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.

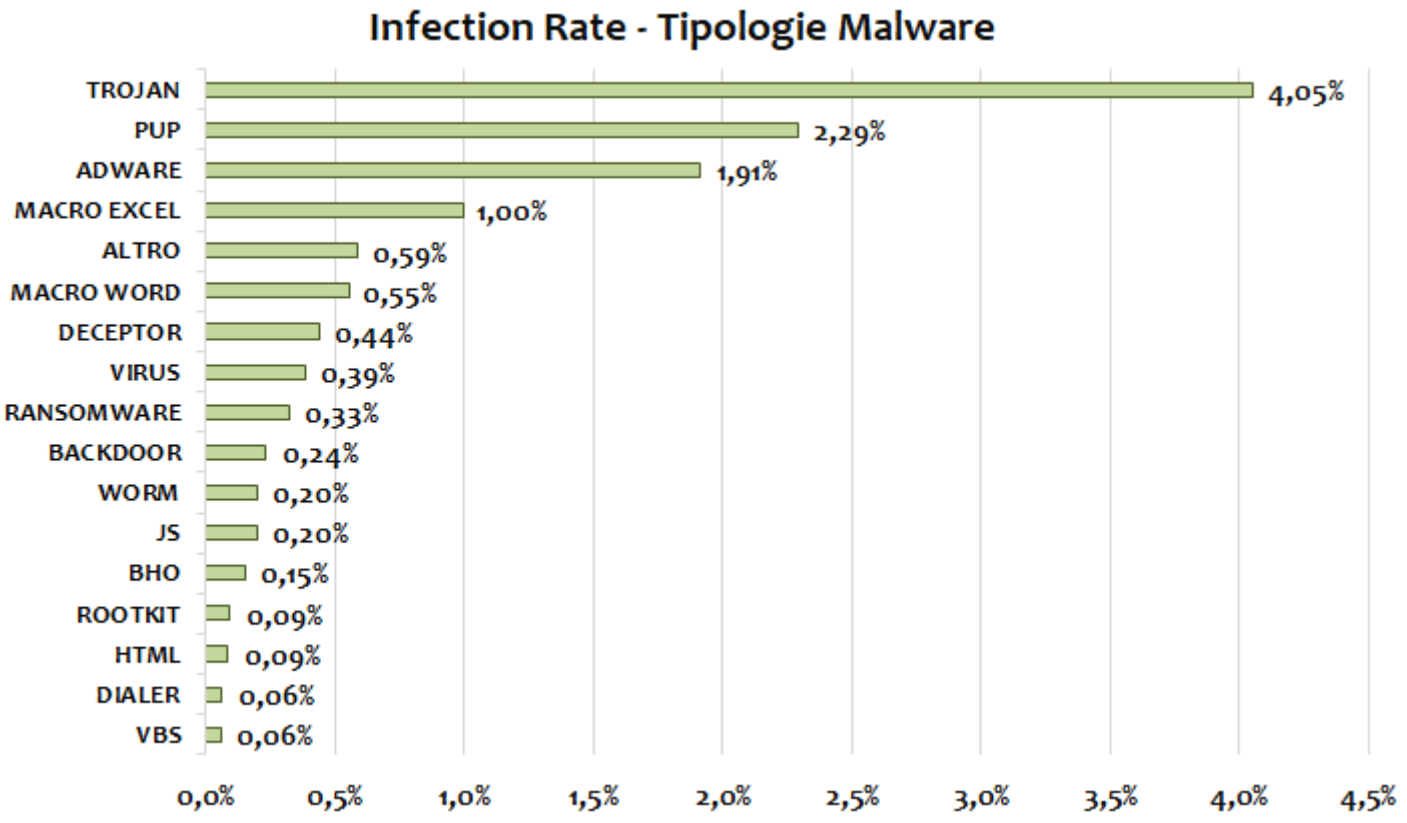
Vediamo ora i dati relativi alla prevalenza dei malware registrati dal C.R.A.M. di TG Soft nel mese di novembre. Per prevalenza si intende l'incidenza che i malware hanno in un determinato periodo. Il valore calcolato si chiama "rate di infezione".

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 4,05%. Secondo posto confermato per i **PUP** , con una percentuale del 2,29%. Terzo gradino del podio per la categoria **Adware** con l'1,91%.

Dalla 4ª alla 6ª posizione troviamo i **MACRO WORD**, seguiti dal gruppo generico denominato **Altro** (che include le macro di Office generiche) e i **MACRO EXCEL**. Si attestano in 9ª posizione i **Ransomware** con lo 0,33% in crescita rispetto al mese scorso. 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.).

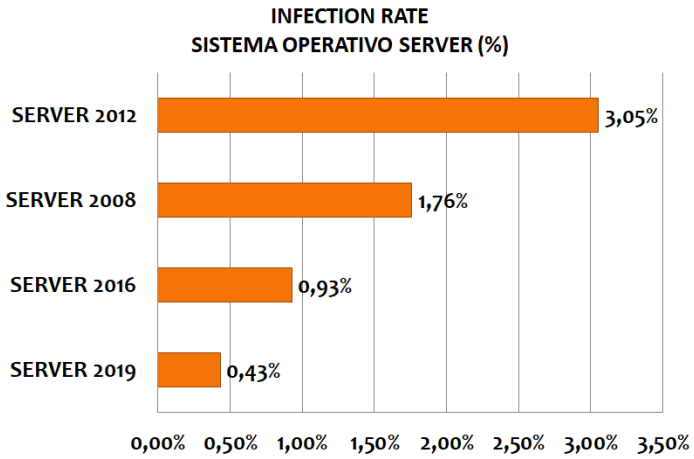


Andiamo ora ad analizzare la prevalenza delle infezioni del mese di novembre in base ai sistemi operativi suddivisi tra sistemi Server e Client.

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.

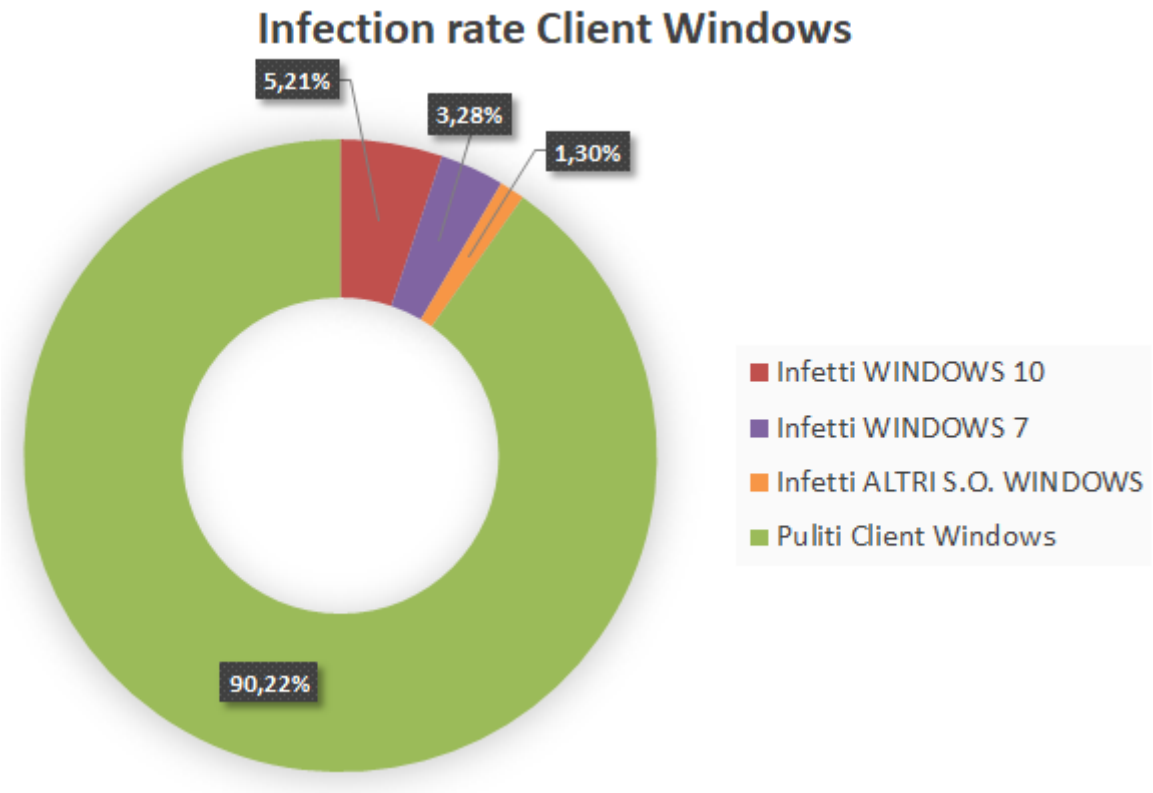
Dai dati relativi ai server, si potrebbe evincere che la probabilità dell'infezione/attacco di un Server 2019 rispetto ad un Server 2012 (più datato…) è di un ordine di grandezza inferiore 0,43% contro 3,05%.

Nelle statistiche relative alla prevalenza delle infezioni dei computer client nel mese di novembre abbiamo riscontrato che il **9,79%** dei terminali è stato infettato o ha subito un attacco. Questo dato indica che **10 computer su 100** sono stati colpiti da malware nel mese di novembre.



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

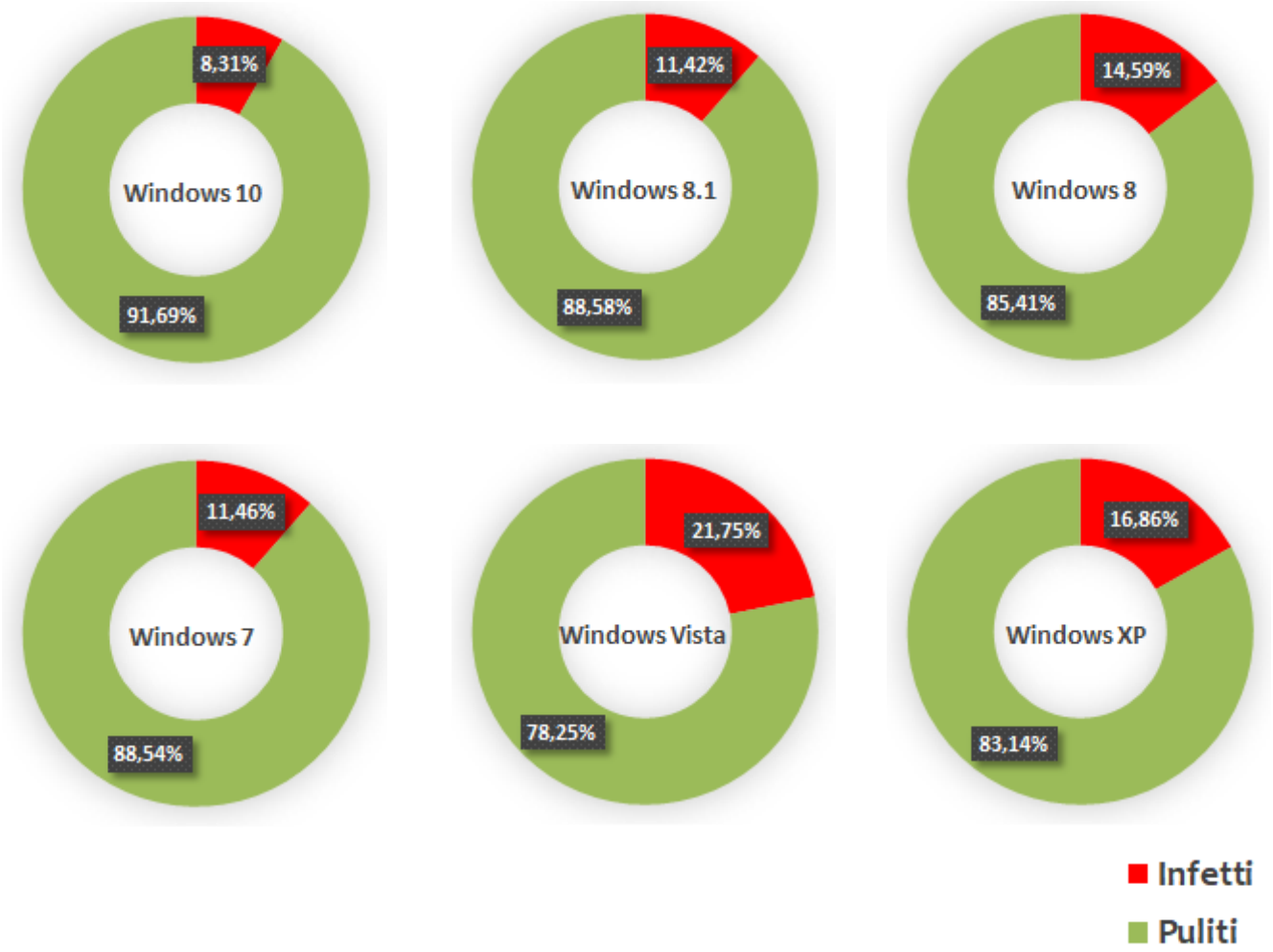
- 62,65% client con Windows 10
- 28,61% client con Windows 7
- 8,74% client con altri s.o. Windows



Windows 10 e **Windows 7** coprono più del 91% del parco macchine dei Client, pertanto gli altri sistemi operativi sono stati raccolti in un unico gruppo.

Ma quale sarà il sistema operativo più sicuro ?

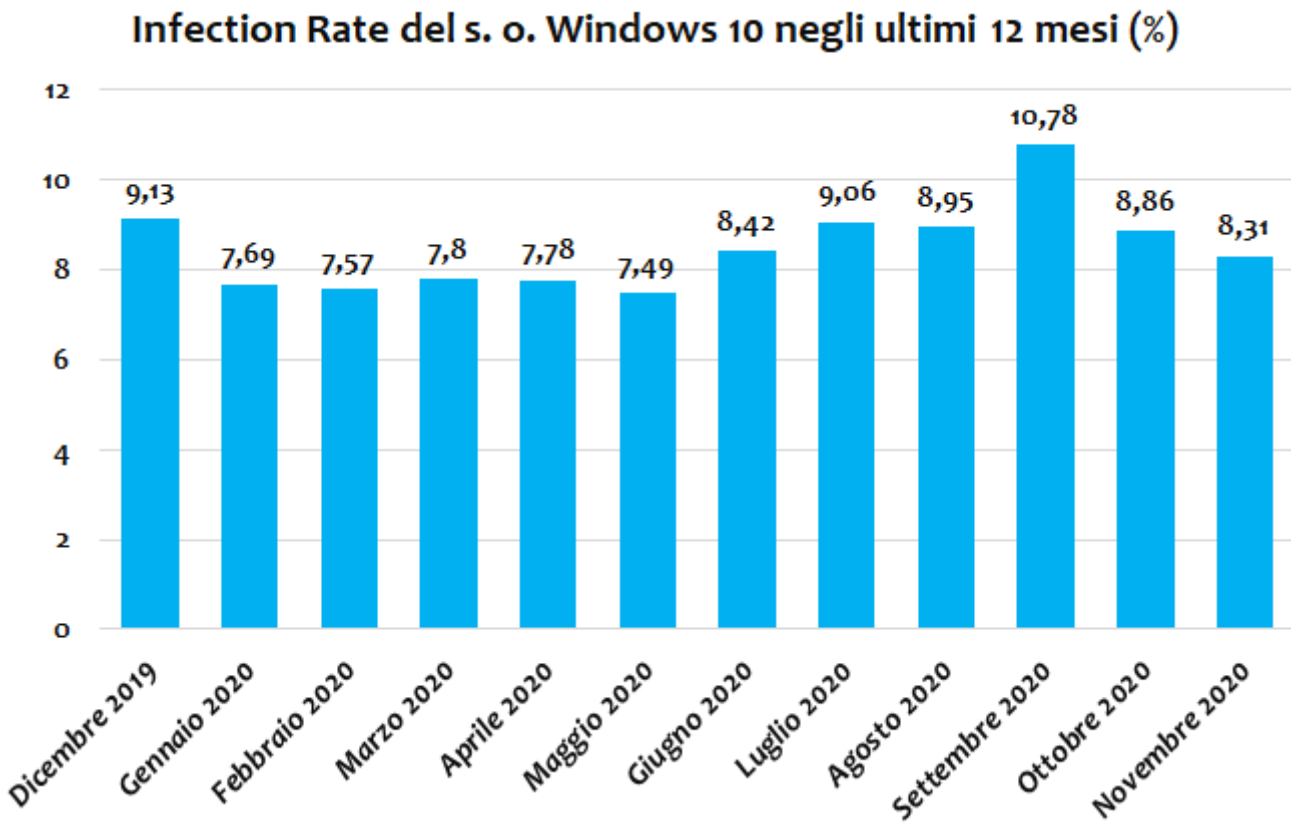
Per rispondere a questa domanda dobbiamo calcolare la prevalenza d'infezione sul medesimo sistema operativo. Prendendo ad esempio Windows 10, si può notare che il rate di infezione tra tutte le macchine ove è installato Windows 10 che ha subito un attacco informatico è del 8,31% . Con questo calcolo 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 XP a Windows 10, si può notare infatti che l'IR è più del doppio.

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

Il periodo di maggiore infezione è stato settembre 2020. In quel periodo si è avuto in Italia una massiva diffusione di campagne malware atte a distribuire il trojan Emotet. Negli ultimi 12 mesi Emotet si è diffuso da dicembre 2019 a fino a metà febbraio 2020, per poi riprendere la sua attività dal mese di luglio 2020. Nel mese di novembre registriamo una leggera flessione del numero di cluster di malware e un decremento del numero delle infezioni rispetto al mese scorso. Questo calo di infezioni è dovuto alla pausa che si è preso Emotet a livello mondiale nel mese di novembre.



TG Soft
Cyber Security Specialist
www.tgsoft.it