Maggio 2020

TG Soft
Cyber-Threat Report

Notizie di rilievo:

Ransomware:
FuckUnicorn

Panorama delle minacce in Italia a Maggio

Il mese di maggio non si è molto scostato dal normale andamento delle campagne malware diffuse in Italia dei mesi precedenti. Nella prima parte del mese si è vista una costante presenza del malware Ursnif assieme a vari password stealer come LokiBot, FormBook, SLoad, AdWind, HawkEye, Ave_Maria e MassLogger. Sono continuati gli attacchi via RDP sebbene in numero più ridotto rispetto ai mesi precedenti, che hanno veicolato i seguenti ransomware: Dharma e LockBit.
Verso la fine del mese è stata veicolata una campagna malspam a tema Coronavirus, che faceva riferimento all'app IMMUNI, atta a diffondere un ransomware presumibilmente di origine italiana, che è stato denominato FuckUnicorn.

CRAM
CENTRO RICERCHE ANTI-MALWARE

Sommario:

TG Soft
Cyber Security Specialist
www.tgsoft.it

TG Soft S.r.l.

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

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

Proteggiamo il tuo business dai cyber-criminali

www.tgsoft.it

TG Soft Cyber Secuirty Specialist è produttore della suite di sicurezza Anti-Virus denominata **Vir.IT eXplorer**. Attiva nel panorama della sicurezza informatica dai primi anni '90.

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

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

Seguici nei social:

Cyber-Threat Intelligence e Infection Rate

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

Il C.R.A.M. (Centro Ricerche Anti-Malware) di TG Soft raccoglie i dati della telemetria inviati dal software anti-virus VirIT eXplorer installato sui propri utenti e le informazioni di investigazione sui casi di attacchi informatici, per tracciare lo stato della Cyber-Security in Italia.

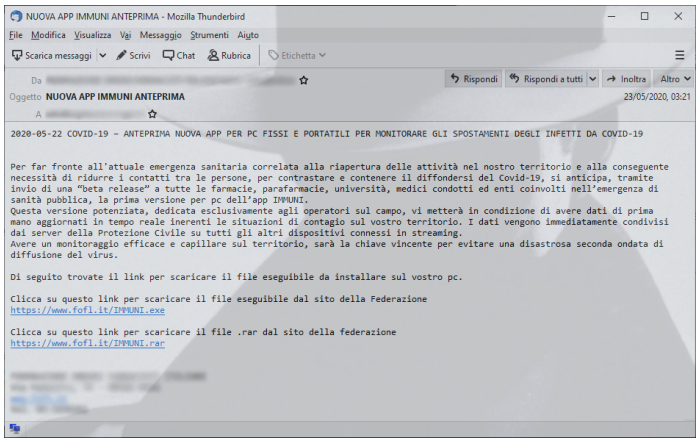
L'indice che misura lo stato della Cyber-Security è l'Infection Rate (IR), che è la percentuale degli utenti dell'anti-virus VirIT eXplorer che hanno incontrato una minaccia ed è stata bloccata e segnalata al C.R.A.M. di TG Soft. L'Infection Rate può essere calcolato su un sotto-insieme di dati, ad esempio su un determinato sistema operativo, fornendoci particolari informazioni e indizi su quale possa essere il sistema operativo 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 ed è stata segnalata al C.R.A.M. di TG Soft"

In primo piano

Ransomware: FuckUnicorn

Il 23 maggio è stata distribuita una campagna malspam in italiano con oggetto "NUOVA APP IMMUNI ANTEPRIMA". Il messaggio invitava ad installare nel proprio PC l'app IMMUNI da un link presente all'interno del messaggio, per far fronte all'attuale emergenza sanitaria dovuta al CoronaVirus. Il link in realtà scaricava il ransomware denominato **FuckUnicorn**.



Analizzando il codice del Ransomware che è stato scritto in linguaggio C# si può subito notare che le estensioni dei file da cifrare sono: .txt, .jar, .exe, .dat, .contact, .settings, .doc, .docx, .xls, .xlsx, .ppt, .pptx, .odt, .jpg, .png, .csv, .py, .sql, .mdb, .sln, .php, .asp, .asp, .html, .htm, .xml, .psd, .pdf, .dll, .c, .cs, .mp3, .mp4, .f3d, .dwg, .cpp, .zip, .rar, .mov, .rtf, .bmp, .mkv, .avi, .apk, .lnk, .iso, .7-zip, .ace,.arj, .bz2, .cab, .gzip, .lzh, .tar, .uue, .xz, .z, .001, .mpeg, .mp3, .mpg, .core, .crproj, .pdb, .ico, .pas, .db, .torrent.

I file da cifrare vengono cercati ricorsivamente all'interno delle seguenti cartelle:

Desktop, Links, Contacts, Documents, Downloads, Pictures, Music, OneDrive, Saved Games, Favorites Searches, Videos.

Di fatto il Ransomware cifra i file contenuti nella cartella profilo dell'Utente (%userprofile%).

I file una volta cifrati avranno questa struttura:

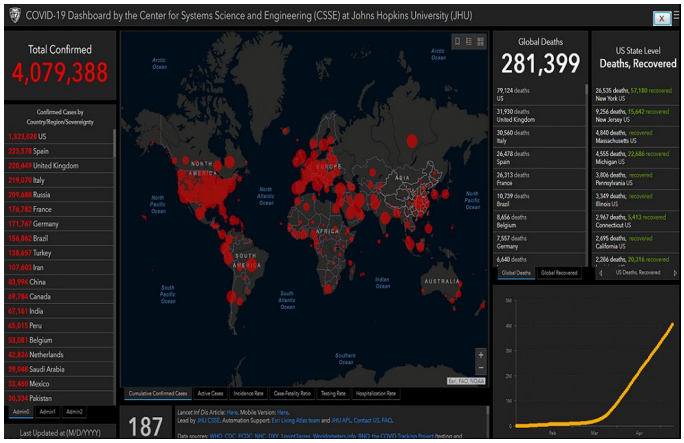
[NOME FILE].[ESTENSIONE].fuckunicornhtrhrtjrjy

IMMUNI.exe

MD5:
b226803ac5a68cd86ecb7c0c6c4e9d00

Dimensione: 978432 Bytes

Mentre il Ransomware cifra i file viene mostrata all'utente la seguente schermata di una mappa raffigurante l'infezione del CoronaVirus:



In seguito viene creato il file con le istruzioni del riscatto in questa cartella: %userprofile%\Desktop\ con nome **READ_IT.txt**.

Il prezzo del riscatto da pagare è di 300 Euro, da versare in cryptovaluta BitCoin al seguente wallet: **195naAM74WpLtGHsKp9azSsXWmBCaDscxJ**

In data 30/06/2020 il Wallet risulta vuoto e non ha mai eseguito alcuna transazione sia in ingresso che in uscita.

Viene inoltre modificato lo sfondo del desktop con un'immagine scaricata dal sito di condivisione immagini https://i.imgur[.]com/6bDNKfs.jpg che vediamo di seguito:

Contenuto del file READ_IT.txt:

La lunga serpe sul bastone di Asceplio si è ribellata, ed una nuova era sta per sopraggiungere! Questa è la vostra possibilità per redimervi dopo anni di peccati e soprusi. Sta a voi scegliere. Entro 3 giorni il pegno pagare dovrai o il fuoco di Prometeo cancellerà, i vostri dati così come ha cancellato il potere degli Dei sugli uomini. Il pegno è di solamente 300 euros, da pagare, con i Bitcoin al seguente indirizzo : 195naAM74WpLtGHsKp9azSsXWmBCaDscxJ dopo che pagato avrai, una email mandarci dovrai. xxcte2664@protonmail.com il codice di transazione sarà la prova. Dopo il pegno pagato riceverai la soluzione per spegnere il fuoco di Prometeo. Andare dalla polizia o chiamare tecnici a niente servirà, nessun essere umano aiutarti potrà.

Il Ransomware invia una serie di informazioni al suo server di Comando & Controllo con la seguente struttura: *http://116.203.210.]127/write.php?computer_name=<NOME PC>&userName=<NOME UTENTE>&password=<STRINGA 15 caratteri>&allow=ransom*

- computer_name: Nome del computer colpito
- userName: Nome utente del computer colpito
- password: Stringa di 15 caratteri randomici utilizzata per generare la chiave AES (Rijndael) per la cifratura dei file
- allow: valore costante impostato a "ransom"

Analizzando il payload del Malware si nota che è presente un PDB:
C:\Users\Leonardo\source\repos\ fuckunicorn\fuckunicorn\obj\Release\IMMUNI.pdb

```
000AC1D0  01 00 00 00 43 3A 5C 55 73 65 72 73 5C 4C 65 6F  ....C:\Users\Leo
000AC1E0  6E 61 72 64 6F 5C 73 6F 75 72 63 65 5C 72 65 70  nardo\source\rep
000AC1F0  6F 73 5C 66 75 63 6B 75 6E 69 63 6F 72 6E 5C 66  os\fuckunicorn\f
000AC200  75 63 6B 75 6E 69 63 6F 72 6E 5C 6F 62 6A 5C 52  uckunicorn\obj\R
000AC210  65 6C 65 61 73 65 5C 49 4D 4D 55 4E 49 2E 70 64  elease\IMMUNI.pd
000AC220  62 00 4A E0 0A 00 00 00 00 00 00 00 00 00 64 E0  b.Jà..........dà
```

Il malware non utilizza tecniche particolarmente sofisticate e sembra essere ancora in una fase embrionale dello sviluppo.

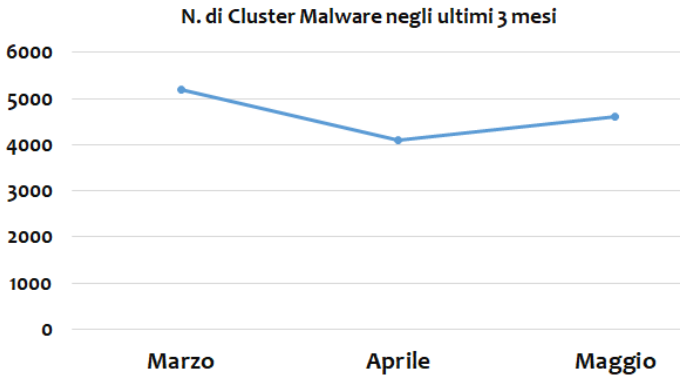
Vi sono però vari indicatori che fanno ipotizzare che la realizzazione del Ransomware sia svolta da Cyber-Criminali di nazionalità Italiana presumibilmente alle prime armi.

Per tutti i clienti con Vir.IT eXplorer PRO il Ransomware FuckUnicorn viene intercettato dalla protezione Euristico Comportamentale Anti-Ransomware protezione Crypto-Malware, maggiori dettagli sono disponibili al seguente link: Tecnologie Anti-Ransomware.

Statistiche Malware

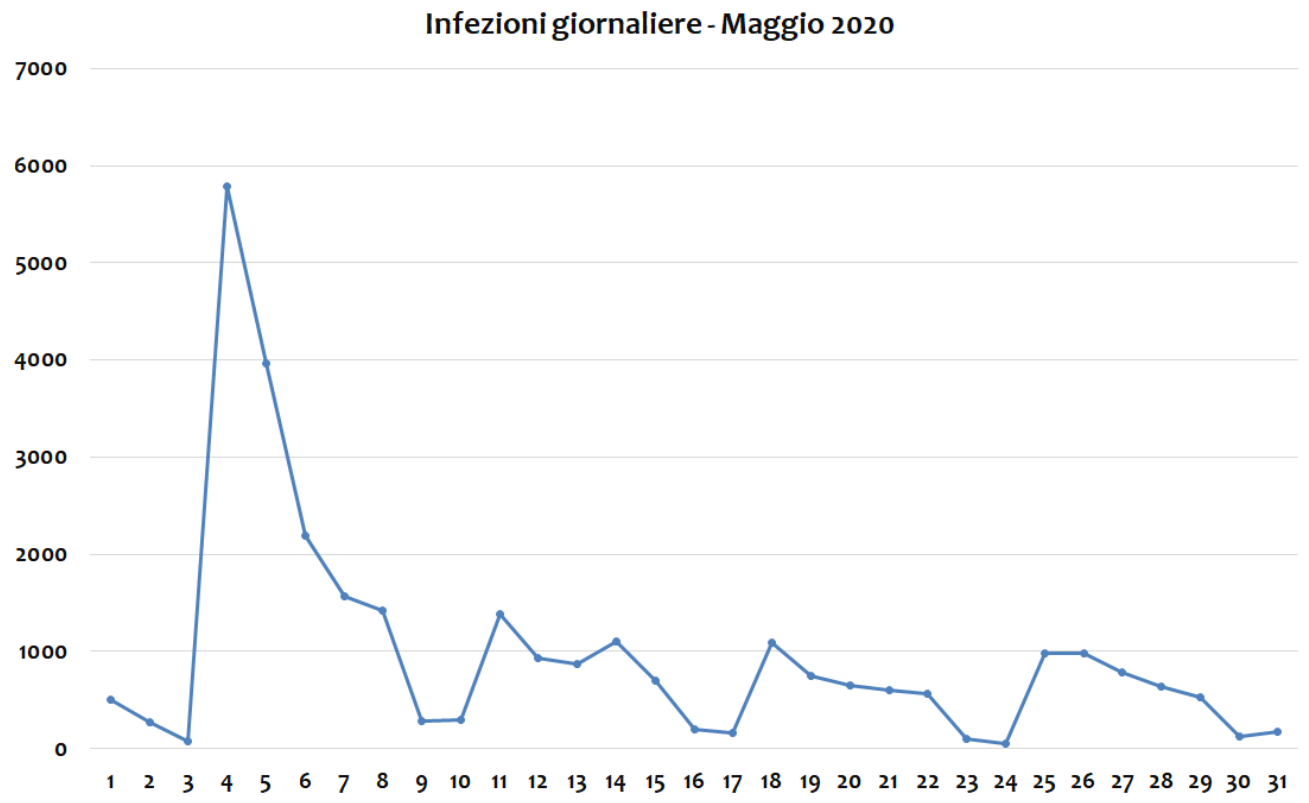
Maggio 2020—ITALIA

I dati della telemetria del C.R.A.M. di TG Soft sono raccolti dagli utenti dove è installato 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 VirI.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 maggio abbiamo avuto un aumento dei malware rispetto al mese scorso di aprile, dove erano stati riscontrati 4091 cluster di malware contro i 4600 del mese di maggio. Questo incremento è sicuramente dato dalla ripresa lavorativa delle società dopo il lockdown in Italia causato da Covid -19.

Nel grafico a fondo pagina possiamo vedere l'andamento giornaliero delle infezioni nel mese di maggio in Italia. All'inizio del mese vi è stato il ponte del 1° maggio, anche se è stato pesantemente condizionato da lockdown imposto a causa del corona virus, si riscontra il punto minimo delle infezioni a maggio. Nella settimana successiva abbiamo un picco di segnalazioni (lunedì 4 maggio) dovute alle scansioni automatiche mensili del motore anti-virus Vir.IT eXplorer. Nelle settimane successive vi è una stabilizzazione delle infezioni riscontrate. Come si può vedere da grafico nei fine settimana vi un calo delle infezioni riscontrate, dovute alla tipologia dell'utenza aziendale e non privata.



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

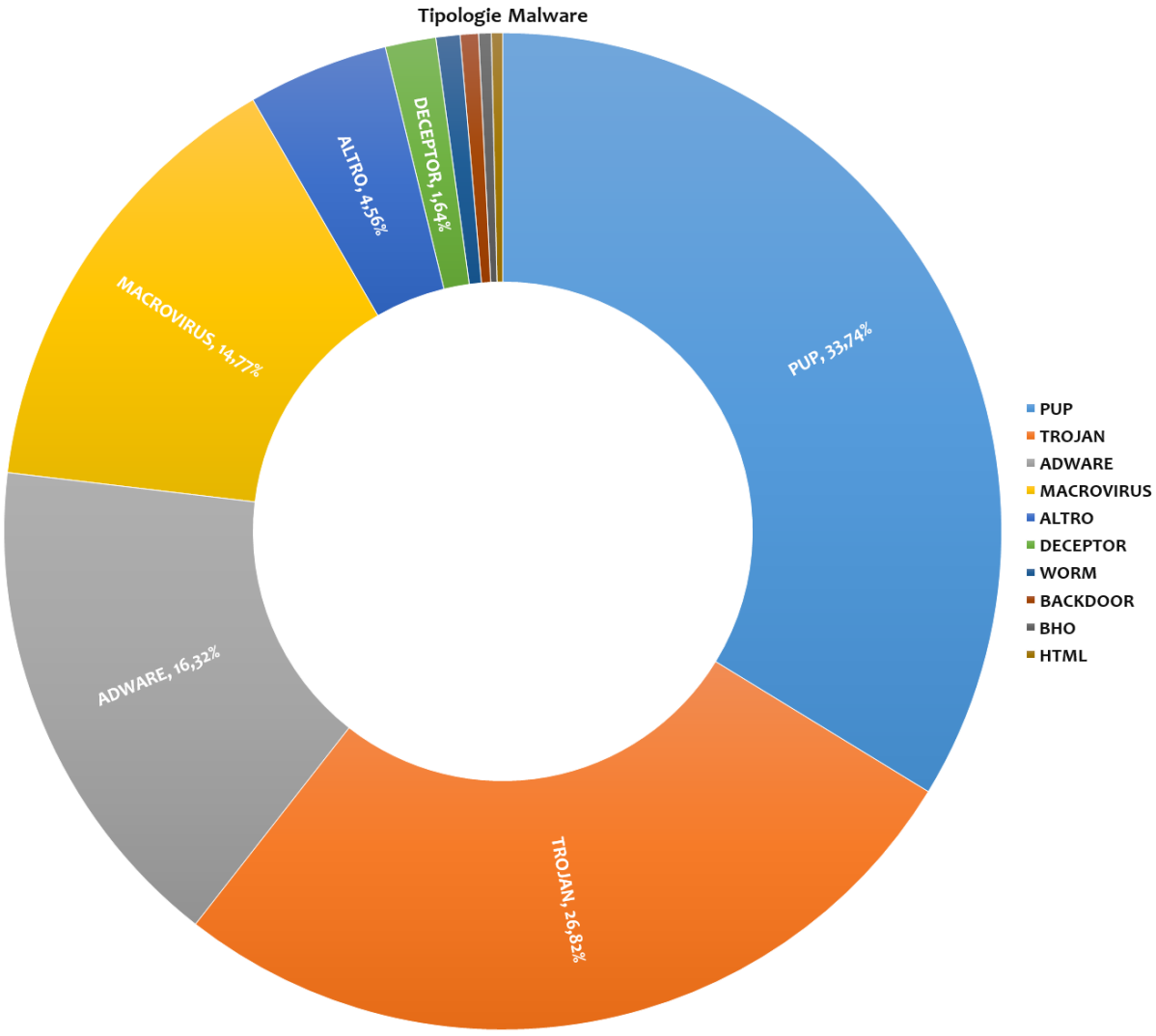
Con il termine malware intendiamo qualsiasi tipologia di software malevolo che possa arrecare danno al sistema informatico.

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

PUP: Potentially Unwanted Program, programmi potenzialmente indesiderati, che di solito sono in "bundle" con software gratuiti.

Nel mese di Maggio si evince una classifica per Tipologia con un podio ben delineato rispetto al mese precedente. Netto il primo posto per i **PUP** che con il 33,74% (+2,99%) superano i **TROJAN** scesi al 26,82% (-3,94%) . Il divario è di oltre cinque punti percentuali. Gli **ADWARE** si riconfermano al terzo posto con un valore pressoché invariato, 16,68% (+0,36%), rispetto alla precedente classifica.

Sale ancora di qualche punto, confermando la quarta posizione, la categoria **MACRO VIRUS**, a maggio raggiunge infatti il 14,77% (+2,87%). Al quinto posto troviamo il gruppo denominato "**ALTRO**" con contengono i virus con il 4,56%. Seguono i **DECEPTOR** con l'1,64%, poi i **WORM**, le **BACKDOOR**, i **BHO** e gli **HTML**.



Analizziamo le statistiche di maggio dei singoli Malware. Il numero di PUP (Potentially Unwanted Program) rimane il più alto con cinque presenze nella TOP10, in vetta troviamo il solito **PUP.Win32.MindSpark** con la sola variante "F", che può compromettere il tuo browser, modificando l'home page e il motore di ricerca.

Per quanto riguarda i TROJAN, si nota una sola presenza nella Top10 e riguarda Il **Trojan.LNK.Dropper.BK** che ad Maggio si piazza in quarta posizione, perdendo l'1,42% rispetto al mese precedente.

Al calo dei TROJAN presenti nella TOP10 si contrappone la presenza di ben tre Virus, sono il virus polimorfico **Win32.Sality.BH** (ottava posizione) , il **Win32.Delf.FE** (nona posizione) e il **Win32.Expiro.AQ** (decima posizione). Va ricordato che queste tipo di minacce infettano i file di tipo eseguibile (applicazioni) ed integrano un polimorfismo particolarmente sofisticato che rende la loro rimozione particolarmente complicata.

Come abbiamo visto ad aprile, si riconfermano nel podio della TOP10 gli **Office.VBA.Macro_Heur** (tipologia MACRO VIRUS) , che troviamo a maggio in seconda posizione con un 3,39% delle infezioni. Si tratta di un dato ottenuto tramite l'analisi euristica e riguardano i file contenenti macro potenzialmente pericolose. I malware della Top10 rappresentano il 21,55% delle infezioni del mese di maggio, il rimanente 78,45% è dato da altri 4590 cluster di malware.

I malware della Top10 rappresentano il 21,55% delle infezioni di maggio, il rimanente 78,45% è dato da altri 4590 cluster di malware.

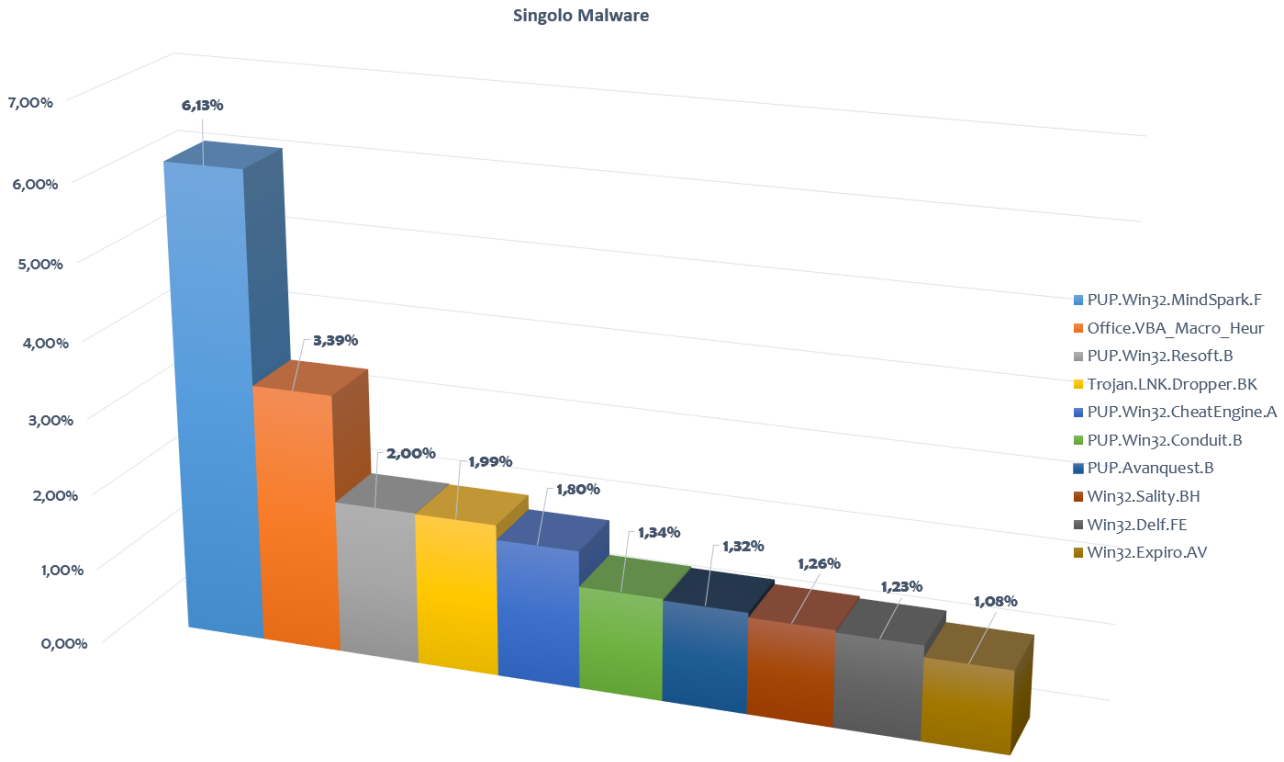
Riepilogando, si sono presentati nella TOP 10 per singolo malware di Maggio le seguenti tipologie:

5 PUP

3 VIRUS

1 MACRO VIRUS

1 TROJAN

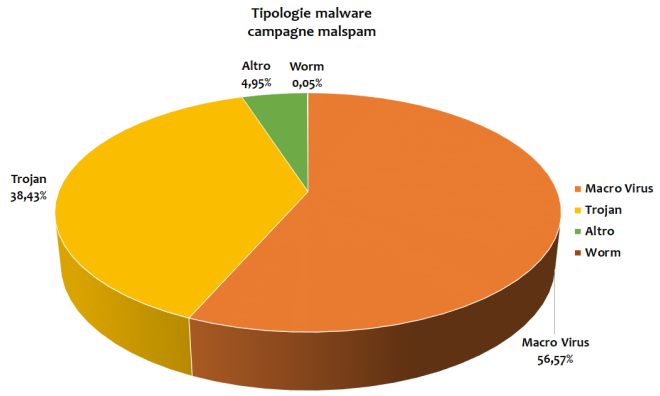


Statistiche Malware via email

Maggio 2020—ITALIA

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

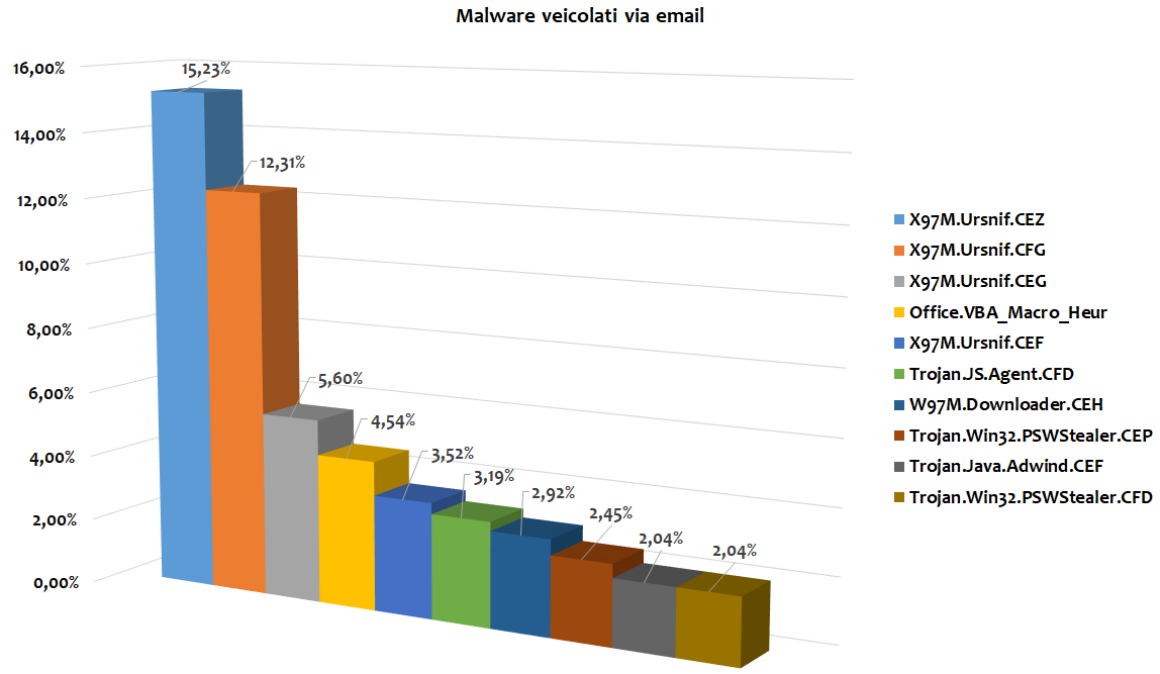
La categoria dei **MACRO VIRUS** mantiene sempre la prima posizione con il 56,57% (-4,30%). Il dato ottenuto, segna una flessione anche nel mese di maggio. Ciò nonostante, la tipologia conserva un ampio margine di vantaggio rispetto alla categoria dei **TROJAN** che con il loro 38,43% (+7,68) si confermano saldamente al secondo posto. Distanziata di oltre trenta punti percentuali, staziona al terzo posto la tipologia **ALTRO** con il 4,95% (+7,10%). Prossima allo zero la tipologia dei **WORM** con lo 0,05%.



Analizziamo le statistiche delle campagne di malspam per singolo malware, si evince anche a maggio un predominante connubio tra i file XLS con macro e il noto malware chiamato **UrSnif**, che occupano il podio della Top10. Le varianti di **X97M.Ursnif** presenti nella Top10 scendono a quattro (erano 7 ad aprile), ma tra i malware appartenenti alla tipologia MACRO VIRUS, troviamo anche un **W97M.Downloader.CEH** (macro virus di Word). Va aggiunto pure il dato ottenuto dall'analisi euristica, che con l'indicatore **Office.VBA_Macro_EUR** (tipologia Macro Virus) raggiunge la quarta posizione.

Completano le rimanenti tre posizioni della classifica, solamente malware della tipologia TROJAN, sono rispettivamente in ordine: il **Trojan.JS.Agent.CFD** (sesta posizione), il **Trojan.Win32.PSWStealer.CEP** (ottava posizione).

il **Trojan.Java.Adwin.CEF** (nona posizione) e per chiudere il **Trojan.Win32.PSWStealer.CED**.



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

Week 21 ==> 23-29/05 2K20 campagne MalSpam target Italia

Week 20 ==> 16-22/05 2K20 campagne MalSpam target Italia

Week 19 ==> 09-15/05 2K20 campagne MalSpam target Italia

Week 18 ==> 02-08/05 2K20 campagne MalSpam target Italia

Ransomware

Maggio 2020—ITALIA

Nel mese di Maggio sono continuati gli attacchi ransomware attraverso l'accesso RDP. Il numero degli attacchi via RDP è diminuito rispetto al mese scorso, molto probabilmente dovuto al fatto che molte aziende hanno ripreso a lavorare direttamente dall'ufficio.

Abbiamo riscontrato attacchi dai seguenti ransomware:

- **Dharma**
- **LockBit**
- **FuckUnicorn**

Nel mese di Maggio ha fatto la sua comparsa un ransomware italiano, che si fa chiamare **FuckUnicorn.**

Sono continuati gli attacchi via RDP, che hanno permesso un accesso abusivo al sistema per eseguire direttamente il ransomware, in questa particolare situazione hanno veicolato il Dharma.

Alcune estensioni dei file cifrati utilizzati dal ransomware Dharma nel mese di maggio:

- **NCOV**
- **EKING**
- **HELP**
- **EJECT**

Anche questo mese troviamo il ransomware **LockBit** attivo negli attacchi RDP in Italia. Sembrerebbe che gli autori del **LockBit** si siano affiliati con quelli del **Maze** per condividere le loro piattaforme di data leak. La richiesta di riscatto del **LockBit** varia dalla tipologia della vittima, potrebbe partire dai 1600 dollari in su.

Prevalenza

Maggio 2020—ITALIA

Quanto sono protetti i computer in Italia a livello di Cyber-Security? 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, quantificandoci la stima dei 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 Maggio 2020. Per prevalenza si intende l'incidenza che i malware hanno in un determinato periodo. Il valore calcolato si chiama "rate di infezione".

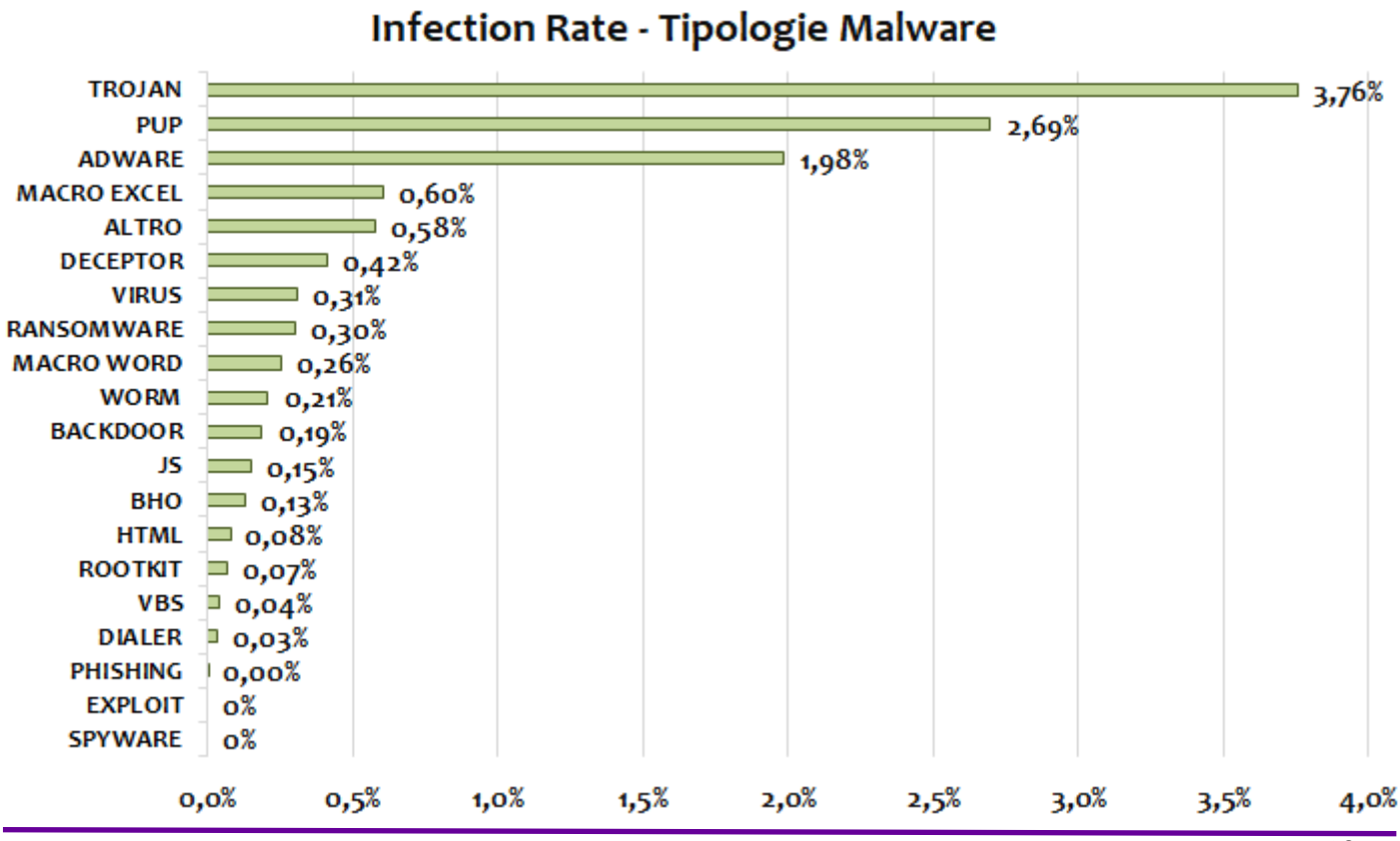
Il rate di infezione viene calcolato dividendo il numero di computer ove siano stati rilevati attacchi per il numero di computer dove è installato il software anti-virus Vir.IT eXplorer. Possiamo calcolare il rate di infezione per le seguenti categorie:

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

Al primo posto i **Trojan** con una percentuale del 3,76%. Secondo posto confermato per i **PUP** , con una percentuale del'2,69%. Terzo gradino del podio per la categoria **Adware** con l'1,98%. Il gruppo generico denominato **Altro** (che include le macro di Office generiche) lascia il quarto posto alla categoria **Macro Excel** con l'0,60%.

Salgono in ottava posizione i **Ransomware** con lo 0,3%. 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, GandCrab, Dharma, Phobos, LockBit etc.) e il vecchio e famoso FakeGDF (virus della polizia di stato, guardia di finanza etc.).



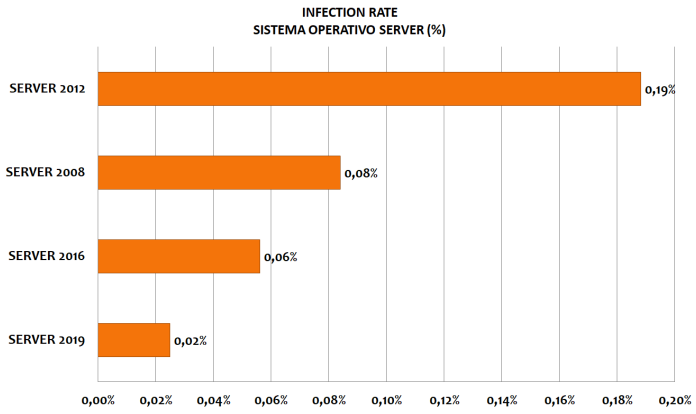
Andiamo ora ad analizzare la prevalenza delle infezioni del mese di Maggio in base ai sistemi operativi suddivisi tra sistemi Server e Client.

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

La classifica dei sistemi operativi server vede quindi in prima posizione Windows Server 2012 (0,19%) seguito da Windows Server2008 (0,08%),

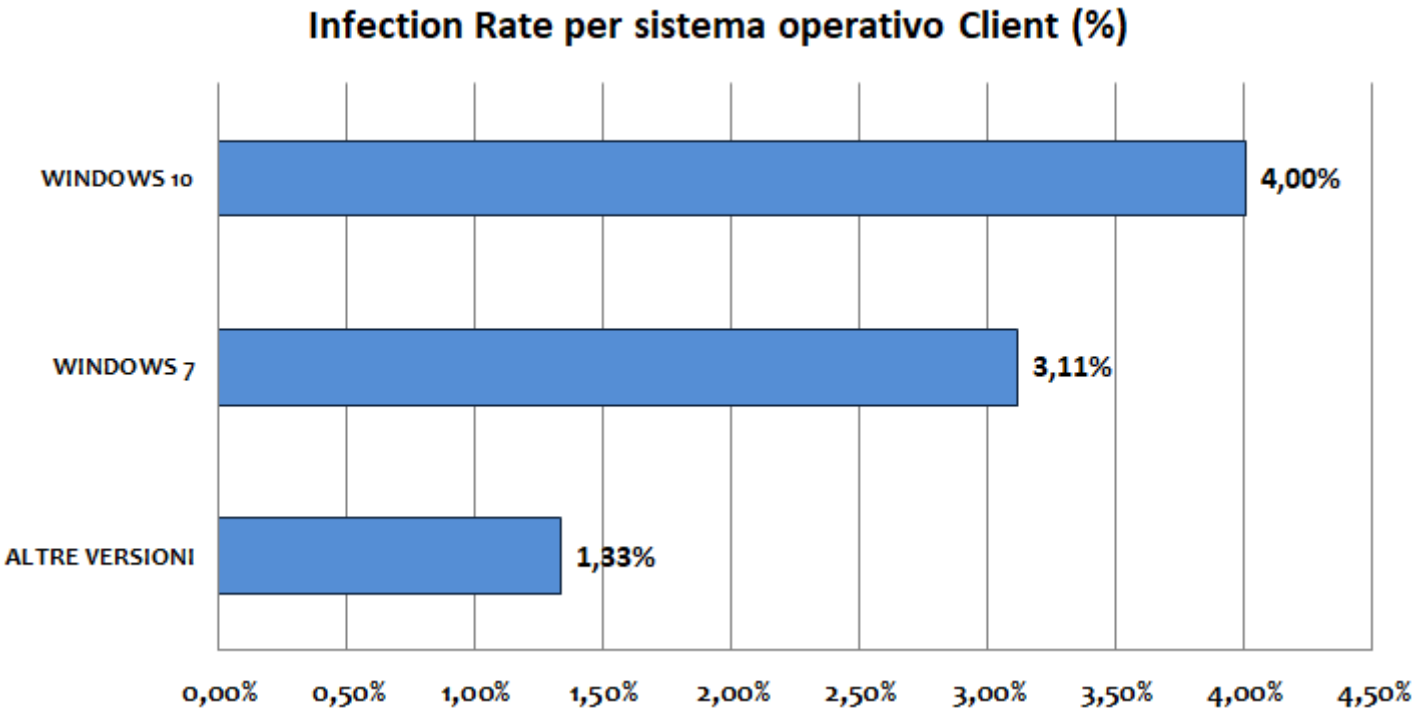
Windows Server 2016 si attesta terzo posto con lo 0,06%. Chiude Windows Server 2019 con lo 0,02%.

Non più in classifica dal 2020 il sistema operativo Windows Server 2003.



Nelle statistiche relative alla prevalenza delle infezioni dei computer client nel mese di Maggio abbiamo riscontrato che circa l'**8,5%** dei terminali è stato infettato o ha subito un attacco. Questo dato indica che **1 computer su 12** è stato colpito da malware nel mese di Maggio.

Nella figura sottostante possiamo vedere il grafico delle infezioni in base ai sistemi operativi dei Client.

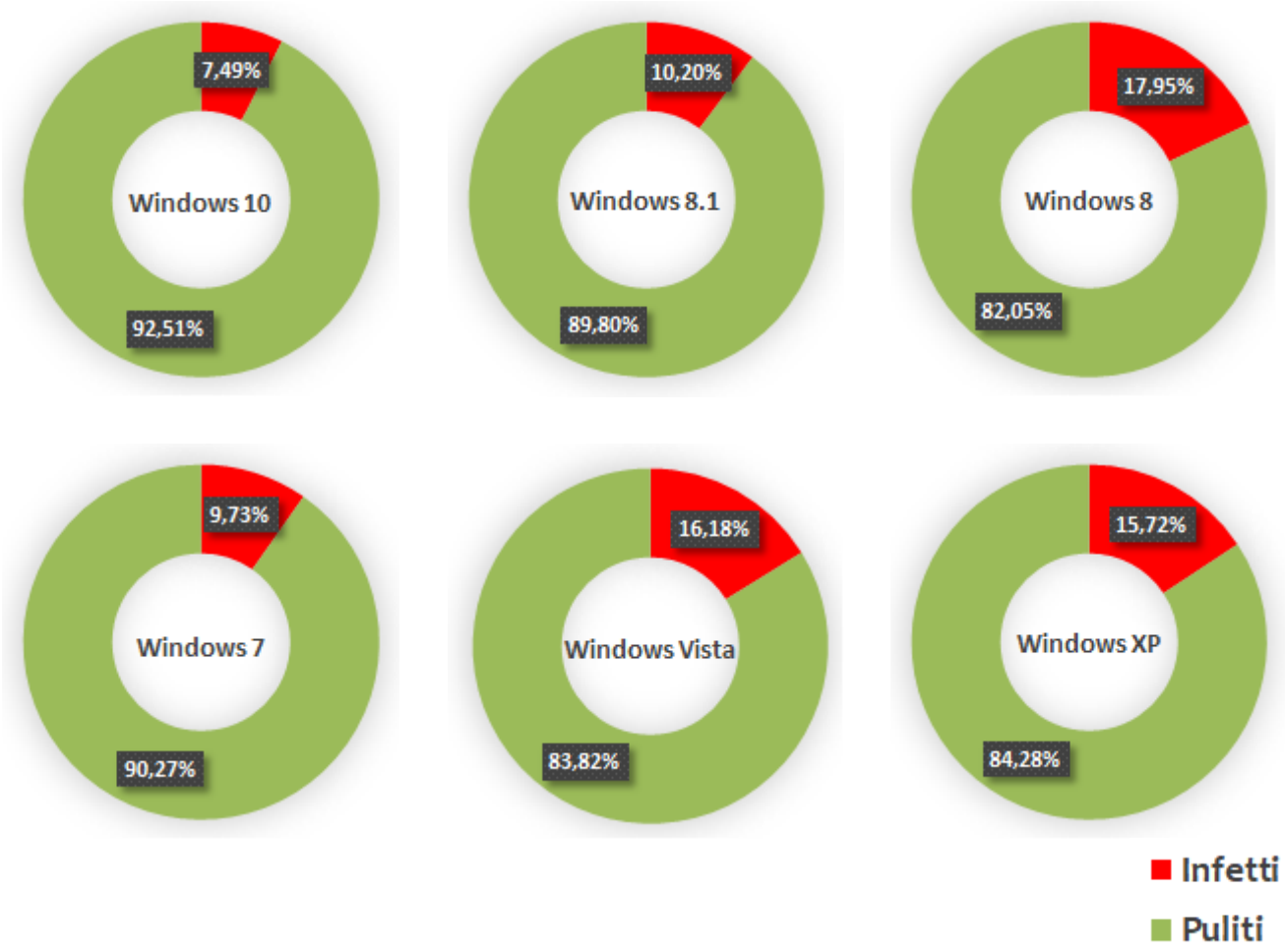


Windows 10 e **Windows 7** coprono quasi l' 88% del parco macchine dei Client, pertanto gli altri sistemi operativi sono stati raccolti in un unico gruppo.

Nel grafico della pagina precedente, relativo ai Client, prima posizione per **Windows 10** con il 4,00%. Secondo **Windows 7** il 3,11%. Gli altri sistemi operativi si attestano di poco sotto il punto e mezzo percentuale ovvero all'1,33%.

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, il 7,49% ha subito un attacco informatico. 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 oltre il doppio.

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

Il periodo di maggiore infezione come è visibile è ottobre 2019, in quel periodo e anche nei mesi adiacenti erano massivamente diffuse campagne malware atte a distribuire i trojan Emotet e TrickBot. Da Gennaio 2020 la situazione a seguito della diminuzione delle campagne di Emotet/TrickBot sembra essersi normalizzata. Anche il mese di maggio rientra nell'andamento standard dei primi mesi del 2020.