Cyber-Threat Report

Giugno 2020

TG Soft
Cyber Security Specialist
www.tgsoft.it

Giugno 2020

TG Soft
Cyber-Threat Report

Notizie di rilievo:

Ransomware: Avaddon

Panorama delle minacce in Italia a giugno

Nel mese di giugno abbiamo avuto un aumento degli attacchi informatici, ma un calo del numero dei cluster di malware rispetto al mese precedente.
Nella prima e nell'ultima parte del mese si è vista una costante presenza del malware Ursnif attraverso campagne di malspam a tema "Agenzia delle Entrate".
Non sono mancati i vari password stealer come HawkEye, Remcos, MassLogger, NanoCore, Ave_Maria, LokiBot, NetWire, AdWind e Azorult. Nella settimana centrale di giugno abbiamo avuto un picco di attacchi di JasperLoader. Sono continuati gli attacchi via RDP che hanno veicolato i seguenti ransomware: Dharma, Kupidon e LockBit.
Un nuovo ransomware denominato Avaddon ha fatto la sua comparsa in Italia veicolato attraverso campagne di malspam dirette o dal malware Phorphiex.

C.R.A.M.
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

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.** 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.

Proteggiamo il tuo business dai cyber-criminali

[www.tgsoft.it]

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/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 VirIT eXplorer che hanno incontrato una minaccia 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, 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

Ransomware: Avaddon

Nel mese di giugno un nuovo ransomware denominato Avaddon ha fatto la sua apparizione in Italia.

I nostri sensori di Cyber-Threat Monitor e tecnologie Anti-Ransomware hanno individuato i seguenti attacchi in Italia nel mese di giugno:

- Martedì 9 giugno
- Mercoledì 10 giugno
- Giovedì 11 giugno
- Mercoledì 17 giugno
- Venerdì 26 giugno
- Martedì 30 giugno

Il ransomware Avaddon utilizza diversi vettori d'infezione per diffondersi:

- Campagne di malspam
- Botnet di Phorphiex

Avaddon

MD5: 4FAC8DF05EE106A9F658B9BB4F90D05

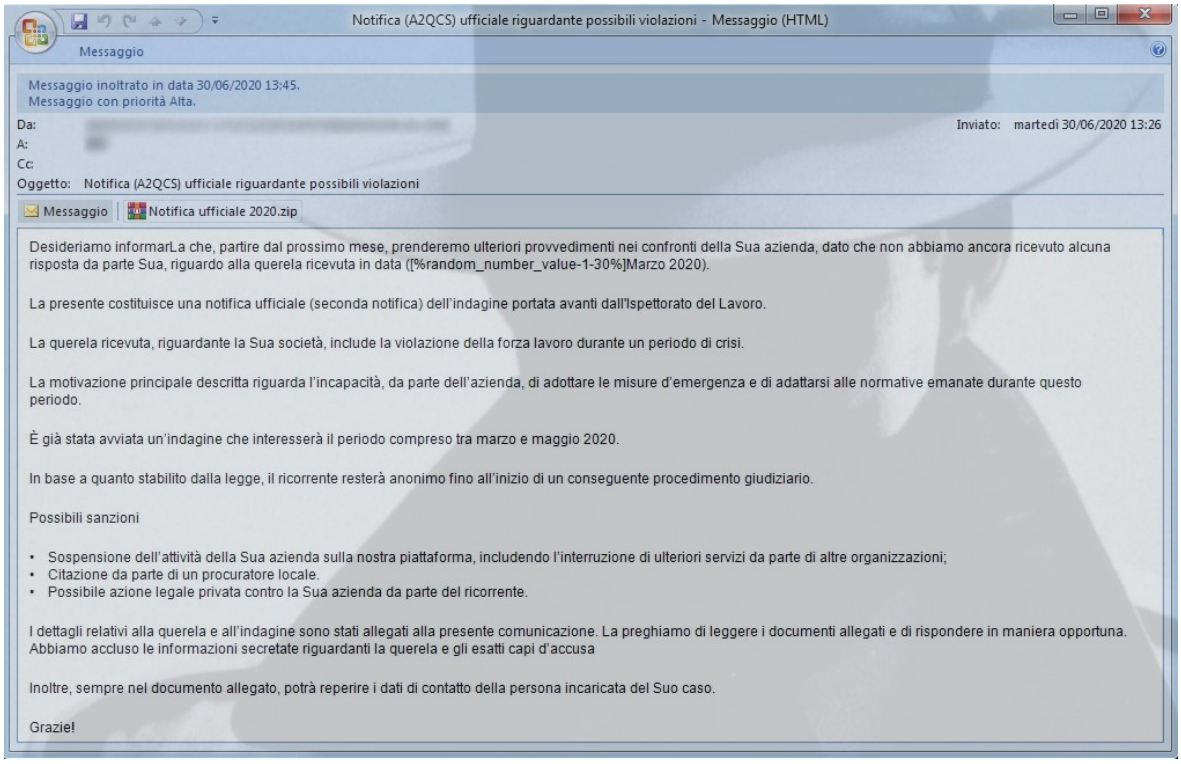
Dimensione: 1.135.616 Bytes

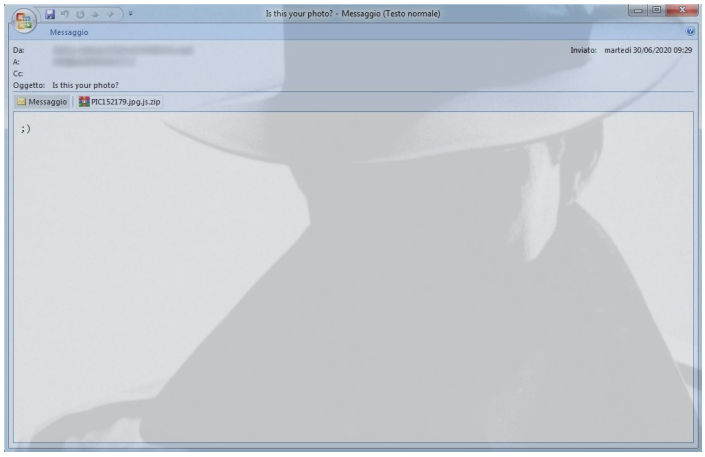
VirIT: Trojan.Win32.CryptAvaddon

Nel mese di giugno abbiamo registrato campagne di malspam dirette sia di Avaddon sia di Phorphiex.

Phorphiex è un malware downloader che può installare nel computer altre tipologie di trojan, in questo caso ha scaricato il ransomware Avaddon.

Il 30 giugno sono state monitorate campagne malspam di Avaddon e Phorphiex. Nella figura sottostante possiamo vedere la campagna dell'Avaddon scritta in ottimo italiano, avente oggetto "Notifica (A2QCS) ufficiale riguardante possibili violazioni" e allegato un file zip contenente un file Excel che poi scaricava il ransomware Avaddon.





Nella figura a fianco possiamo vedere invece la campagna malspam di Phorphiex. Il messaggio con oggetto in inglese e il corpo contenente i caratteri a rappresentare una faccina che ti fa l'occhiolino, con allegato un file zip contenente un javascript che scaricherà il malware Phorphiex.

Non siamo a conoscenza se vi è un collegamento diretto tra gli autori di Avaddon e Phorphiex.

Avaddon è un ransomware emergente che sta prendendo piede attraverso attacchi diffusi via email diretti o attraverso la complicità di altri malware.

Avaddon, è un ransomware che, similmente ad altri esegue i seguenti step durante l'attacco:

1. Generazione della chiave di cifratura
2. Chiusura/arresto di una serie di servizi
3. Cancellazione delle SHADOWCOPY e dei punti di ripristino
4. Cifratura dei file
5. Richiesta riscatto

La generazione della chiave di cifratura dei file avviene chiamando la funzione **CryptGenKey**, dove viene creata una chiave **AES casuale a 256 bit**.

Per cifrare la maggior parte dei file, Avaddon arresta una serie di servizi elencati nella figura a fianco.

DefWatch
ccEvtMgr
ccSetMgr
SavRoam
dbsrv12
sqlservr
sqlagent
Intuit.QuickBooks.FCS
dbeng8
sqladhlp
QBIDPService
Culserver
RTVscan
vmware-usbarbitator64
vmware-converter
VMAuthdService
VMnetDHCP
VMUSBArbService
VMwareHostd
sqlbrowser
SQLADHLP
sqlwriter
msmdsrv
tomcat6
QBCFMonitorService

La cancellazione delle Shadowcopy e dei punti di ripristino avviene utilizzando i seguenti comandi:

- wmic.exe SHADOWCOPY /nointeractive
- wbadmin DELETE SYSTEMSTATEBACKUP
- bcdedit.exe /set {default} recoveryenabled No
- bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures
- vssadmin.exe Delete Shadows /All /Quiet

All'interno del ransomware Avaddon è presente una stringa in Base64 che contiene una chiave pubblica **RSA a 2048 bit.** La chiave pubblica RSA a 2048 bit è utilizzata per cifrare la chiave AES a 256 bit generata da **CryptGenKey.**

Inoltre Avaddon contiene all'interno una seconda chiave **AES a 256 bit** che è utilizzata per cifrare la struttura dati json di configurazione del ransomware.

Nella figura a fianco possiamo vedere il json di configurazione di Avaddon, che contiene i seguenti campi:

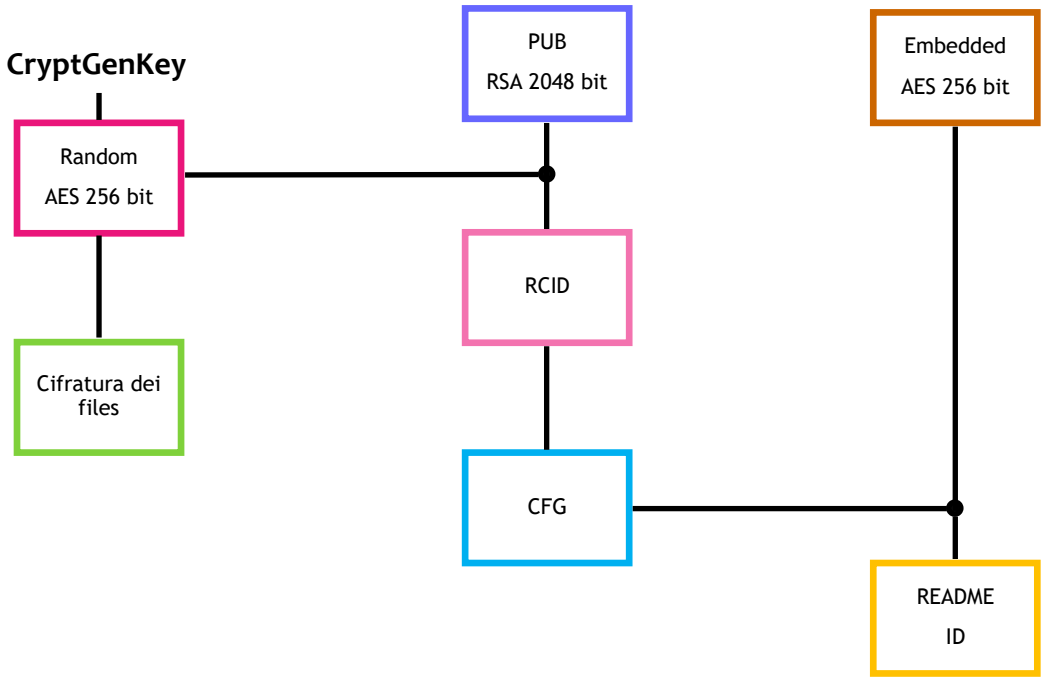
- **ext:** estensione dei file cifrati
- **ip:** indirizzo ip della vittima (ottenuto da api.myip.com)
- **rcid:** stringa esadecimale che contiene l'ID della vittima
- **hdd:** struttura dati che contiene informazioni sulle unità
    a) *name*: lettera dell'unità
    b) *size*: dimensione in GB
    c) *type*: indica se l'unità è locale o remota (lan)
- **lang:** linguaggio del sistema operativo
- **name:** nome del computer

```
{
  "ext": "",
  "ip": "",
  "rcid": "",
  "hdd":
    [
      {  "name": "",
         "size": ,
         "type": ""
      },
    ],
  "lang": "",
  "name": ""
}
```

Il parametro rcid è una stringa esadecimale lunga 1024 caratteri, corrispondenti a 512 byte.

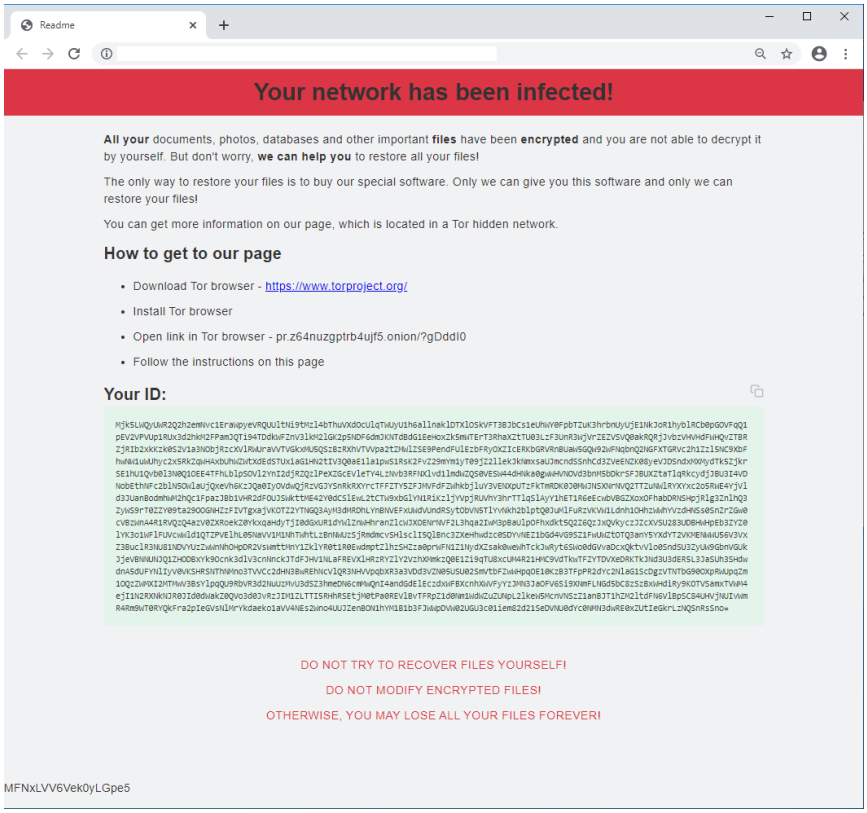
Tutti i file verranno cifrati con la medesima chiave generata da **CryptGenKey** attraverso l'algoritmo **AES a 256 bit** con la modalità **CBC.**

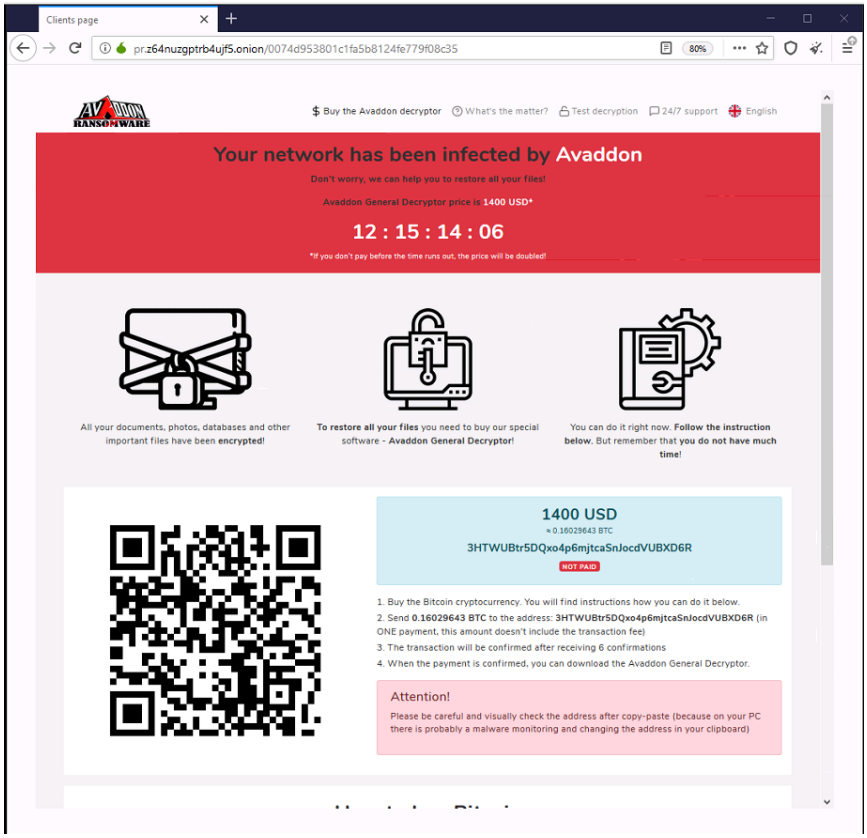
Nella figura sottostante possiamo vedere lo schema riassuntivo di cifratura.



Al termine viene creato sul desktop il file G_readme.html contenente le istruzioni del riscatto con l'ID della vittima.

Il riscatto richiesto è di 1400 $ (dollari USD) da pagare in BTC (bitcoin) entro il countdown, altrimenti il prezzo raddoppierà.





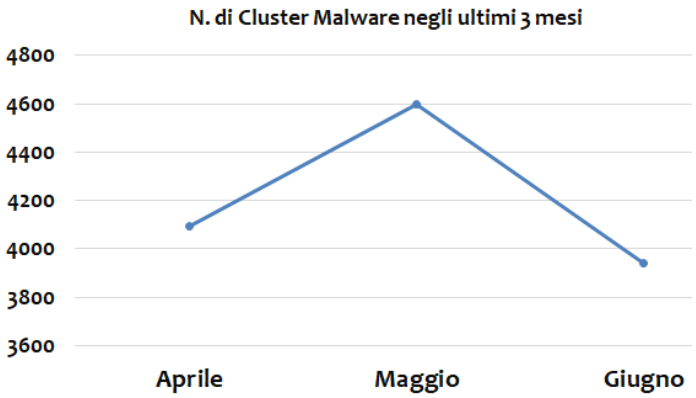
Statistiche Malware

Giugno 2020—ITALIA

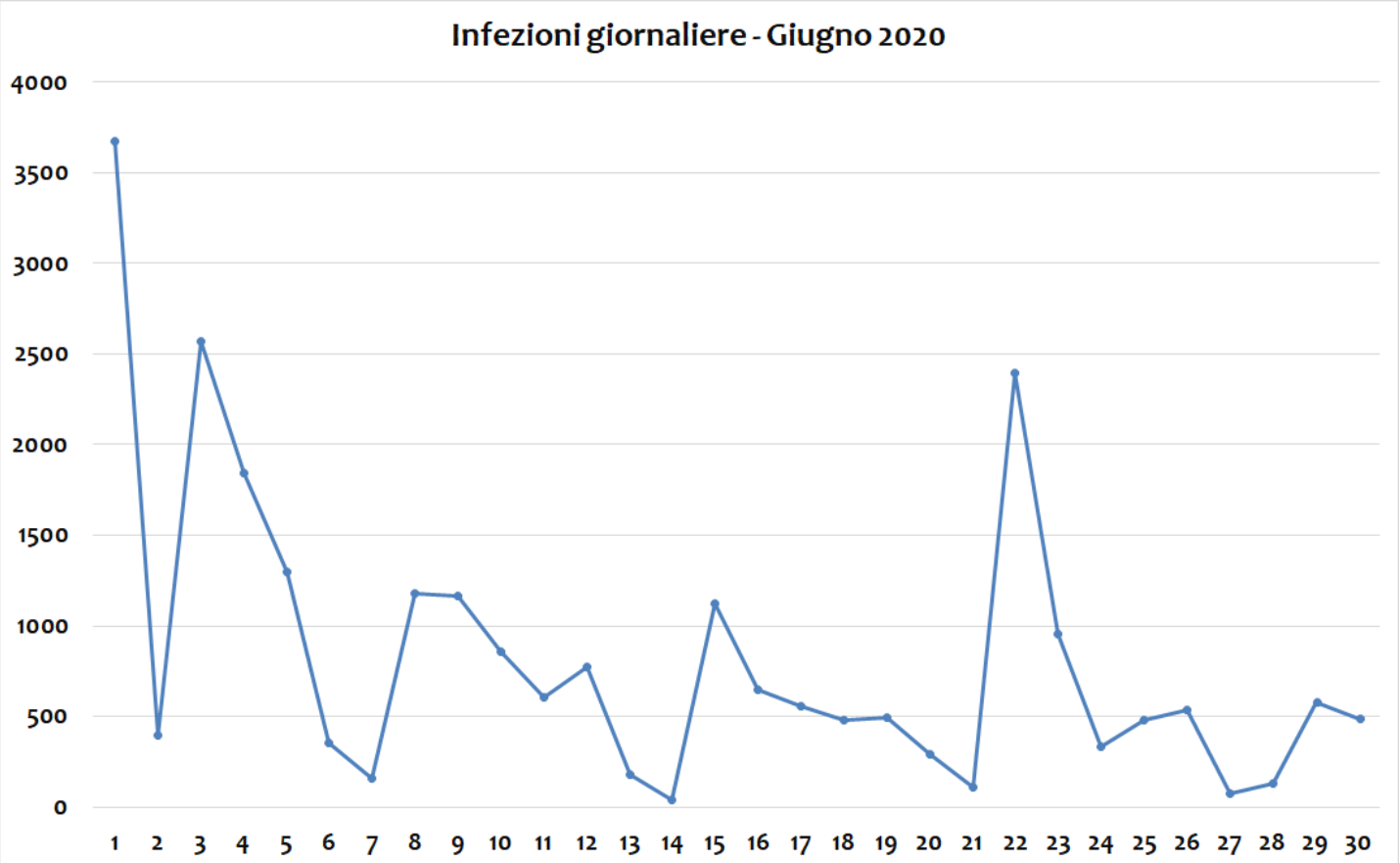
I dati della telemetria del C.R.A.M. di TG Soft sono raccolti dagli utenti che utilizzano il software anti-virus Vir.IT eXplorer. Le segnalazioni derivano da attacchi bloccati oppure malware riscontrati all'interno del parco macchine monitorato. Ogni minaccia identificata da Vir.IT viene classificata 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 giugno abbiamo avuto una diminuzione dei malware rispetto al mese scorso di maggio, dove erano stati riscontrati 4600 cluster di malware contro i 3938 del mese di giugno. Questo decremento potrebbe essere dovuto al periodo estivo di giugno e al raggruppamento progressivo di più malware nello stesso cluster.

Nel grafico a fondo pagina possiamo vedere l'andamento giornaliero delle infezioni nel mese di giugno in Italia. All'inizio del mese abbiamo avuto due picchi di segnalazioni d'infezione, lunedì 1° giugno e mercoledì 3 giugno, dovute alle scansioni automatiche mensili del motore anti-virus Vir.IT eXplorer. Un terzo picco è avvenuto lunedì 22 giugno per dopo decrescere fino alla fine del mese.



Nelle settimane intermedie vi è una stabilizzazione delle infezioni rilevate. Nei fine settimana vi è un calo delle infezioni riscontrate, dovute alla tipologia dell'utenza aziendale che nei fine settimana, generalmente, è molto meno operativa.



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

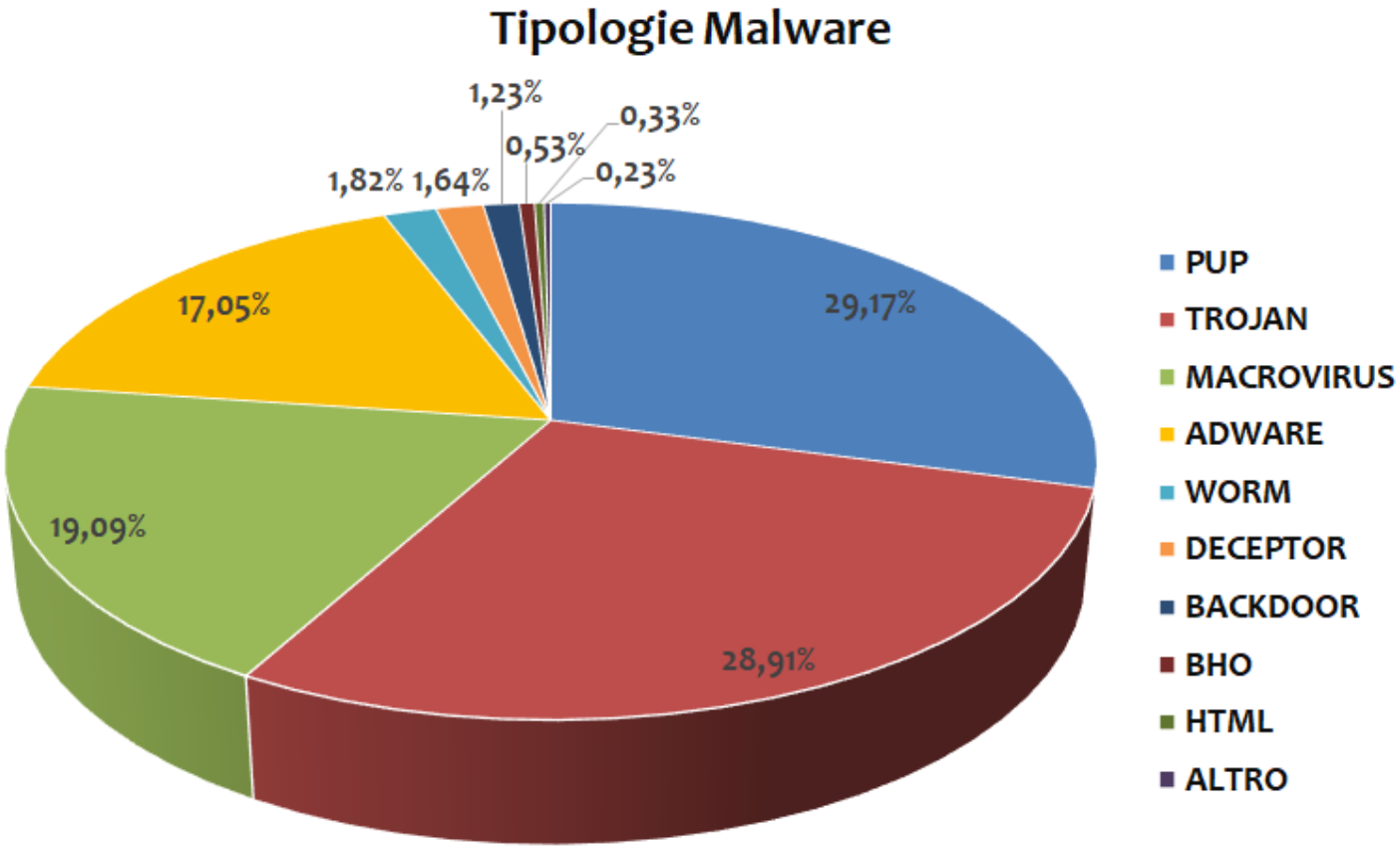
Con il termine malware intendiamo qualsiasi tipologia di software malevolo che possa arrecare danno al sistema informatico.

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

Nel mese di giugno la tipologia dei **PUP/PUA** si mantiene al primo posto con il 29,17% delle infezioni, anche se in calo del 4,47% rispetto al mese precedente. Al secondo posto troviamo la tipologia dei **TROJAN** con il 28,91%, in crescita del 2,09% rispetto a maggio, che solamente per qualche decimo percentuale non ruba la prima posizione ai **PUP**. Al terzo posto troviamo la famiglia dei **MACROVIRUS** con un'importante 19,09%, grazie all'incremento del 4,32% rispetto a maggio guadagna una posizione. Gli **ADWARE** scendono dal terzo al quarto posto con un 17,05% nonostante l'incremento dello 0,73% rispetto a maggio. E' interessante notare che le prime 4 tipologie di malware rappresentano il 94% delle infezione monitorate.

Al quinto posto troviamo gli **WORM** con l'1,82% delle infezioni, seguite dai **DECEPTOR** con l'1,64%, poi seguono **BACKDOOR**, **BHO** e **HTML**.

> ***MACROVIRUS: sono costituiti dalle macro malevoli di Office e di altri software, che possono scaricare altri malware. Negli anni '90 erano catalogati come virus, perché potevano diffondersi infettando altri documenti.***



Analizziamo le statistiche di giugno dei singoli Malware. Il numero di PUP (Potentially Unwanted Program) rimane il più alto con quattro 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.

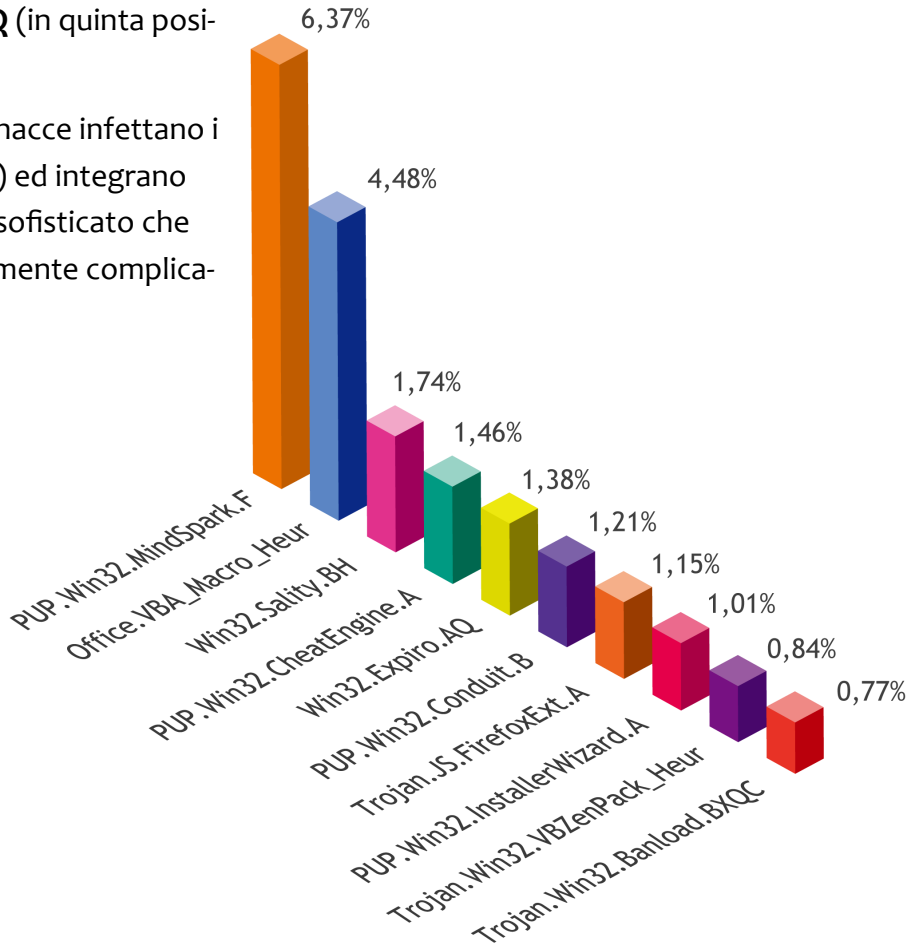
Per quanto riguarda i TROJAN, troviamo tre presenze nella TOP10 e riguardano il **Trojan.JS.FirefoxExt.A** (estensione malevola di Firefox) che a giugno si piazza in settimana posizione, seguono il **Trojan.Win32.VBZenPack_Heur** (offuscatore di codice scritto in VisualBasic usato in questo caso per "proteggere" questo malware) e il **Trojan.Win32.Banload.BXQC** (downloader collegato alla famiglia dell'adware DealPly).

Anche questo mese nella TOP10 troviamo due vecchie conoscenze del mondo dei virus, sono il virus polimorfico **Win32.Sality.BH** (che balza al terzo posto) e il **Win32.Expiro.AQ** (in quinta 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.

I malware della Top10 rappresentano il 20,41% delle infezioni di giugno, il rimanente 79,59% è dato da altri 3928 cluster di malware.

Come abbiamo visto a maggio, si riconfermano nel podio della TOP10 gli **Office.VBA.Macro_Heur** (tipologia MACRO VIRUS) , che troviamo a giugno in seconda posizione con un 4,48% 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 20,41% delle infezioni del mese di giugno, il rimanente **79,59%** è dato da altri 3928 cluster di malware.

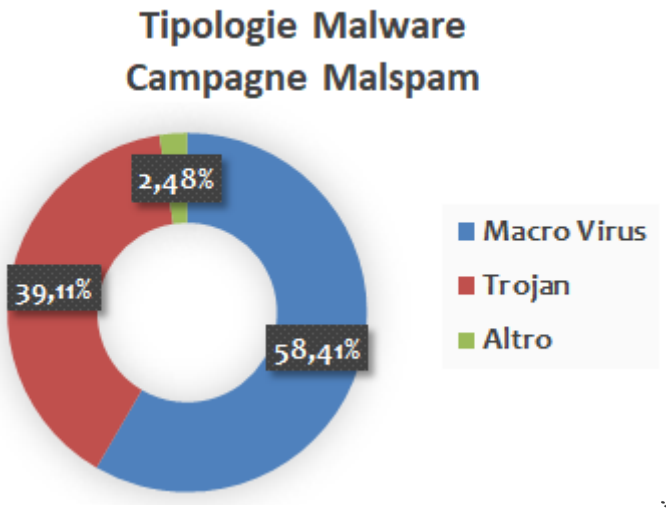


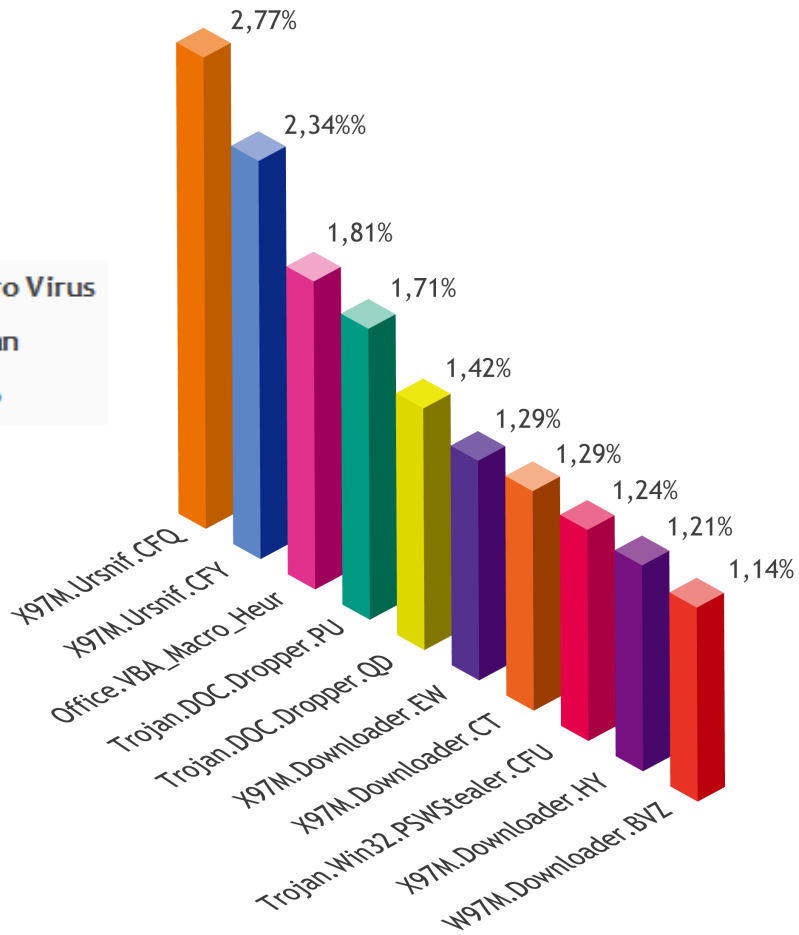
Statistiche Malware via email

Giugno 2020—ITALIA

Analizziamo ora le campagne di malware veicolate via email nel mese di giugno. 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 58,41% (+1,84%). Il dato ottenuto, segna un leggero incremento rispetto a maggio. Seguono la tipologia dei **TROJAN** che con il loro 39,11% (+0,68) si confermano saldamente al secondo posto. Distanziata di oltre trenta punti percentuali, staziona al terzo posto la tipologia **ALTRO** con il 2,48% (-2,47%) che include varie tipologie come **WORM**, **BACKDOOR** e **PHISHING**.





Analizzando le statistiche delle campagne di malspam per singolo malware, si evince anche a giugno un predominante connubio tra i file XLS con macro e il noto trojan bancario chiamato **Ursnif**, che occupano le prime due posizioni del podio della TOP10. Le varianti di **X97M.Ursnif** presenti nella TOP10 scendono a due (erano 4 a maggio), ma tra i malware appartenenti alla tipologia MACRO VIRUS, troviamo anche tre **X97M.Downloader** e un **W97M.Downloader.BVZ** (macro virus di Word). Va aggiunto pure il dato ottenuto dall'analisi euristica, che con l'indicatore **Office.VBA_Macro_EUR** (tipologia Macro Virus) occupa la terza posizione, salendo di un gradino rispetto a maggio.

Completano le rimanenti tre posizioni della classifica, solamente malware della tipologia TROJAN, sono rispettivamente due **Trojan.DOC.Dropper** (quarta e quinta posizione) e il **Trojan.Win32.PSWStealer.CFU** in ottava posizione.

Ursnif

Analisi delle campagne di giugno

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

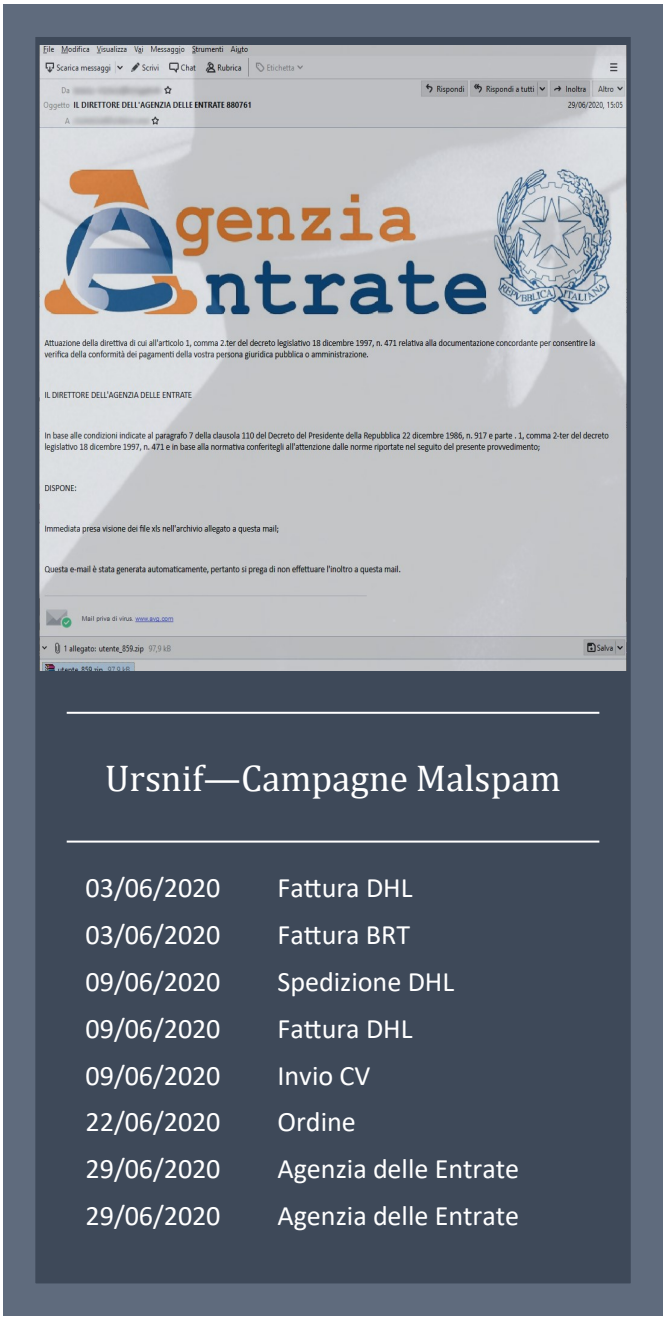
Come abbiamo visto, questo è il malware più diffuso via email in Italia e, a giugno, è stato veicolato attraverso almeno 8 campagne di malspam.

Come si può vedere dalla figura a fianco, l'andamento delle campagne è un po' anomalo. Nella prima settimana di giugno abbiamo rilevato due campagne di malspam nella stessa giornata di mercoledì 3 giugno.

Nella settimana successiva, quella che va da lunedì 8 a domenica 14, vi sono state ben 3 campagne distinte, ma tutte concentrate nella stessa giornata di martedì 9.

Nella settimana da lunedì 15 a domenica 21 non abbiamo campagne Ursnif, sembrerebbe che questo "buco" sia stato colmato dal malware **JasperLoader** con 3 campagne: rispettivamente lunedì 15; mercoledì 17; giovedì 18 giugno.

Le campagne che veicolano Ursnif ritornano lunedì 22 giugno, sfruttando il tema dell'ordine inviato e lunedì 29 giugno utilizzando il "triste" tema dell'Agenzia delle Entrate.



Possibile collegamento tra i cyber-criminali che diffondono campagne malspam in Italia di Ursnif e di JasperLoader.

Analizzando le varie settimane del mese di giugno, ci potrebbe essere un collegamento tra i gruppi dei cyber-criminali che distribuiscono campagne Ursnif e JasperLoader, infatti quando è presente il trojan bancario Ursnif non troviamo il password stealer JasperLoader e viceversa. Potrebbe essere solamente una strana coincidenza oppure, i cyber-criminali che stanno martellando l'Italia da parecchi mesi e utilizzano Ursnif e JasperLoader, o sono i medesimi, o potrebbe esserci una qualche collaborazione.

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

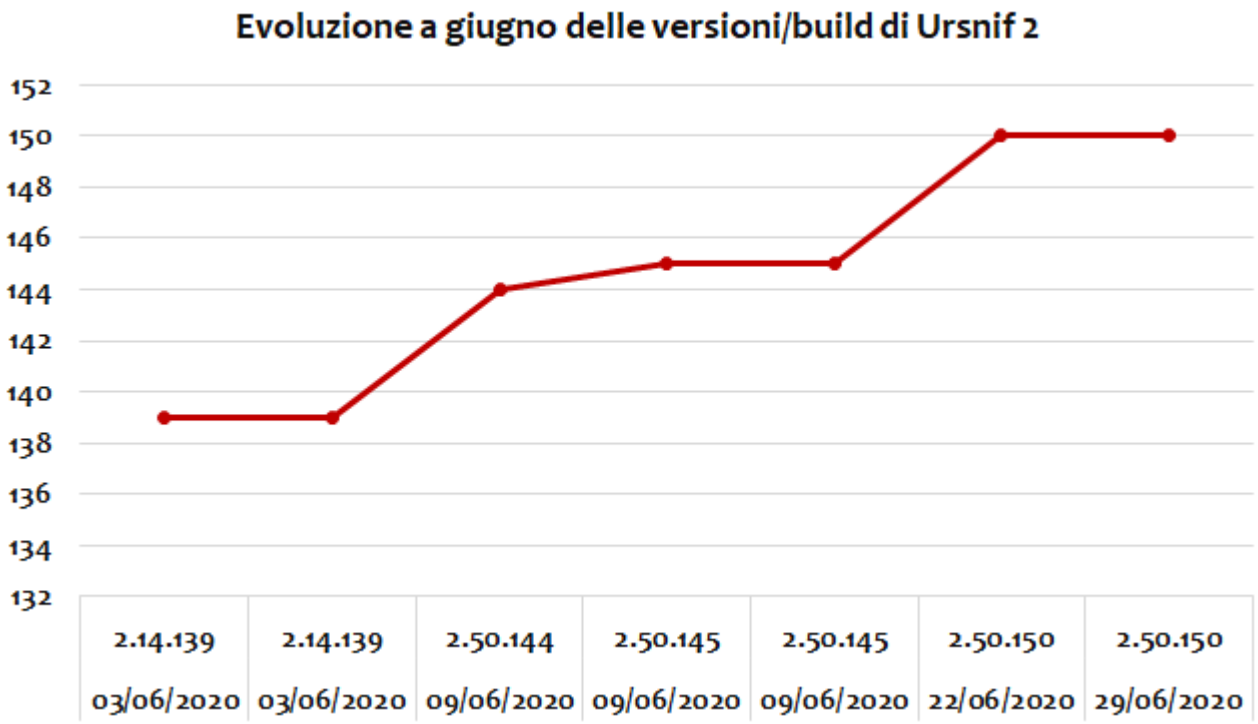
- Versione 2
- Versione 3

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

Nel grafico sottostante possiamo vedere l'evoluzione dello sviluppo del trojan banker Ursnif utilizzato negli attacchi in Italia. Nell'ascissa abbiamo la data della campagna di malspam e la corrispondente versione utilizzata di Ursnif. Nell'ordinata abbiamo la build di sviluppo del malware Ursnif.

E' interessante notare che dal 3 al 9 giugno vi è stato un aggiornamento della versione di Ursnif passando dalla 2.14 alla 2.50.

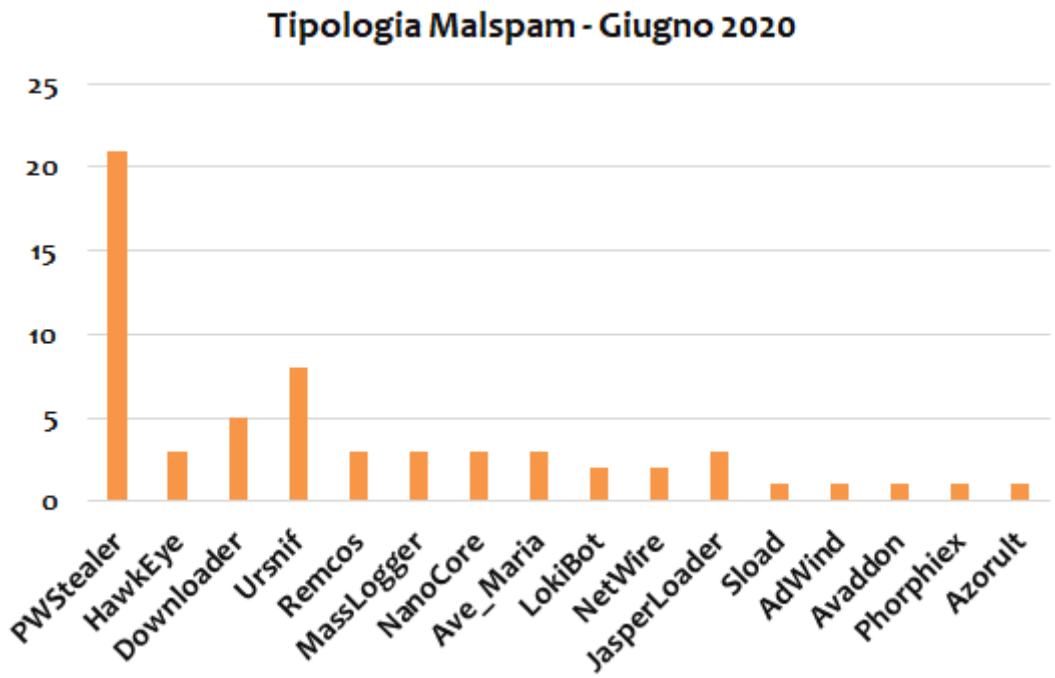
Da questo grafico possiamo vedere la frequenza di rilascio delle varie build di Ursnif.



Analisi dei malware di giugno

Nel mese di giugno in Italia, attraverso le campagne di malspam che hanno "targettizzato" l'utenza italiana (email scritte in lingua italiana), sono stati veicolati 16 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 giugno.



Sono state monitorate più di 20 campagne di **Password Stealer generici**, che hanno lo scopo di rubare le credenziali memorizzate nei browser e della posta elettronica..

Il trojan banker **Ursnif** nel mese di giugno è stato veicolato in 8 campagne di malspam, lo scopo di questo malware è di rubare le credenziali di accesso all'home banking per svuotare il conto corrente. Ursnif in base al gruppo cyber-criminale che lo utilizza può attaccare i conti correnti delle banche italiane, i provider di posta elettronica o i portali come Amazon.

Nel mese di giugno sono stati monitorati altri password stealer o rat come:

- HawkEye
- Remcos
- MassLogger
- NanoCore
- Ave_Maria
- LokiBot
- NetWire
- AdWind
- Azorult

Tutti queste tipologie di malware hanno lo scopo di rubare le password, le informazioni riservate dal computer della vittima o spiarlo.

MassLogger è un password stealer recente, che il C.R.A.M. aveva già iniziato a monitorare in Italia dal 27 maggio.

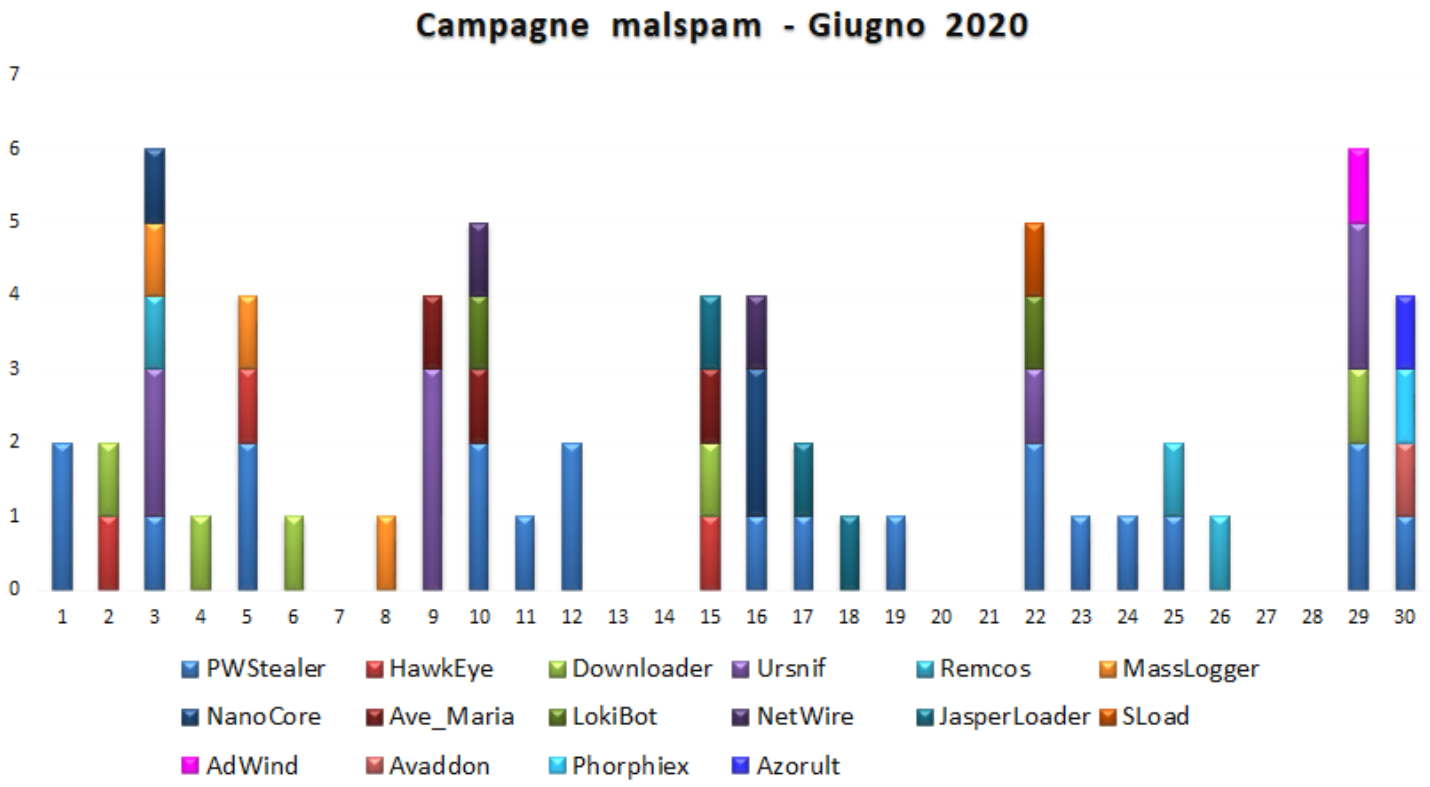
Nella settimana del 15 giugno abbiamo avuto diverse campagne del **JasperLoader**, che ha lo scopo di rubare le credenziali o scaricare altri malware come il **Gootkit** e il ransomware **FTCode.**

Sempre a giugno abbiamo avuto campagne del ransomware **Avaddon** e del downloader **Phorphiex**.

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

Nel mese di giugno abbiamo avuto 2 picchi:

- 3 giugno
- 29 giugno



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

Week 22 ==> dal 30 maggio al 5 giugno

Week 23 ==> dal 6 al 12 giugno

Week 24 ==> dal 13 al 19 giugno

Week 25 ==> dal 20 al 26 giugno

Week 26 ==> dal 27 giugno al 3 luglio

Ransomware

Giugno 2020—ITALIA

Continuano gli attacchi ransomware utilizzando differenti vettori d'infezione.

Questo mese ha fatto la comparsa in Italia un nuovo ransomware denominato **Avaddon**, che ha utilizzato differenti metodi per attaccare l'utenza italiana.

Anche questo mese il numero degli attacchi via RDP è diminuito rispetto al mese scorso, molto probabilmente dovuto al fatto che molte aziende hanno ridotto lo smartworking rientrando a lavorare in sede.

Sono invece aumentate le campagne di malspam che preparano il terreno per gli attacchi ransomware.

La nostra telemetria ha registrato gli attacchi dei seguenti ransomware:

- **Dharma**
- **Kupidon**
- **Avaddon**
- **LockBit**

Il nuovo ransomware Avaddon ha utilizzato diversi vettori d'infezione per attaccare l'utenza italiana:

- Phorpiex
- Campagne malspam dirette

Phorpiex è un worm, che si è diffuso in Italia attraverso campagne di malspam nel mese di giugno. Le vittime infettate entrano a far parte della botnet Phorpiex, che può distribuire il ransomware Avaddon .

Il 30 giugno Avaddon è stato distribuito con una campagna malspam diretta che aveva per oggetto "*Notifica (A2QCS) ufficiale riguardanti possibili violazioni*", con allegato un documento Excel che scaricava il ransomware.

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 **Dharma**.

Alcune estensioni dei file cifrati utilizzati dal ransomware Dharma, rilevati nel mese di giugno sono: **.PGP.**

Un'altra new entry tra i ransomware che hanno attaccato l'Italia nel mese di giugno è **Kupidon**.

L'attacco del Kupidon analizzato è avvenuto attraverso un'intrusione via RDP. Il riscatto richiesto dal Kupidon è 1200 $ (dollari USD) in BTC (Bitcoin). La gang dei cyber-criminali che ha utilizzato Kupidon in questo attacco, potrebbero essere di origine russa dall'indirizzo email (yandex.ru) visibile nell'home page del sito dei malfattori.

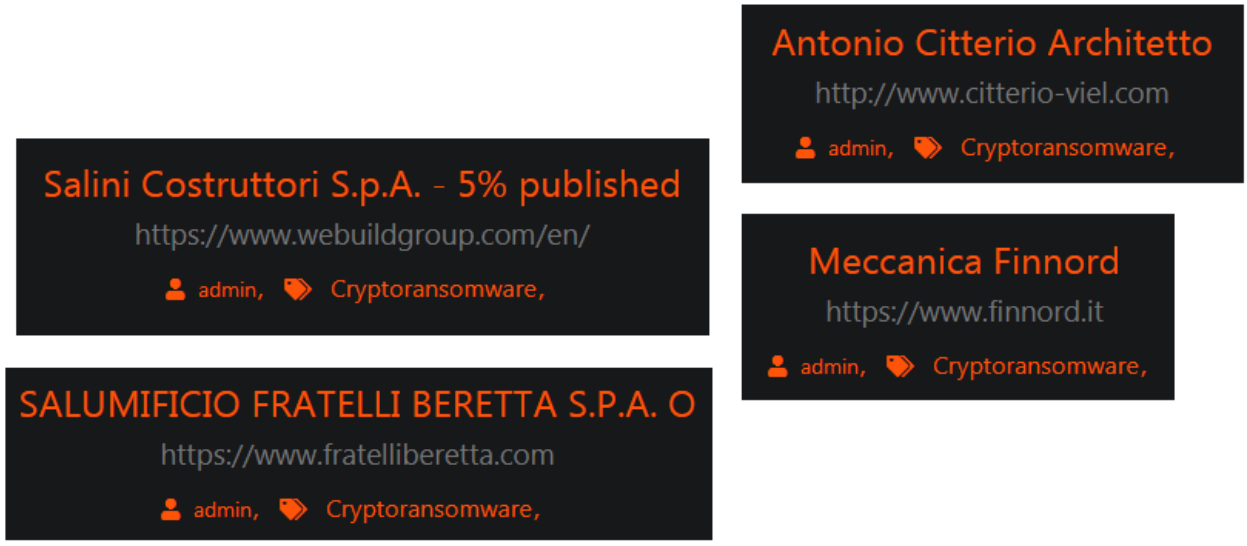
Anche questo mese troviamo il ransomware **LockBit** attivo negli attacchi RDP rilevati in Italia.

Come abbiamo segnalato nel report di maggio, i cyber-criminali di LockBit, sembra, si siano affiliati a quelli del **Maze** per condividere nella loro piattaforma i data leak.

Salgono a quattro le vittime italiane del ransomware Maze:

- Antonio Citterio Architetto
- Salini Costruttori S.p.A.
- Meccanica Finnord
- SALUMIFICIO FRATELLI BERETTA S.P.A.

A livello mondiale Maze recentemente ha colpito anche grandi produttori elettronici come LG e Xerox.



I media italiani hanno riportato gli attacchi ransomware a due grandi società italiane:

- Enel
- Geox

Enel è stata attaccata domenica 7 giugno dal ransomware **Snake/Ekans**, che in precedenza aveva colpito la multinazionale giapponese Honda. Il gruppo che utilizza il ransomware Snake/Ekans, sembra essere interessato ai sistemi industriali di controllo (ICS) e potrebbe essere collegato ad un altro ransomware denominato **MegaCortex,** noto per essere stato utilizzato in passato per l'attacco a grandi multinazionali.

Invece per l'attacco subito da Geox domenica 14 giugno non sono state rilasciate informazioni sulla tipologia di ransomware utilizzato.

Come si può notare la maggior parte degli attacchi ransomware con accesso via RDP avvengono nel fine settimana.

Prevalenza

Giugno 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, 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 giugno 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:

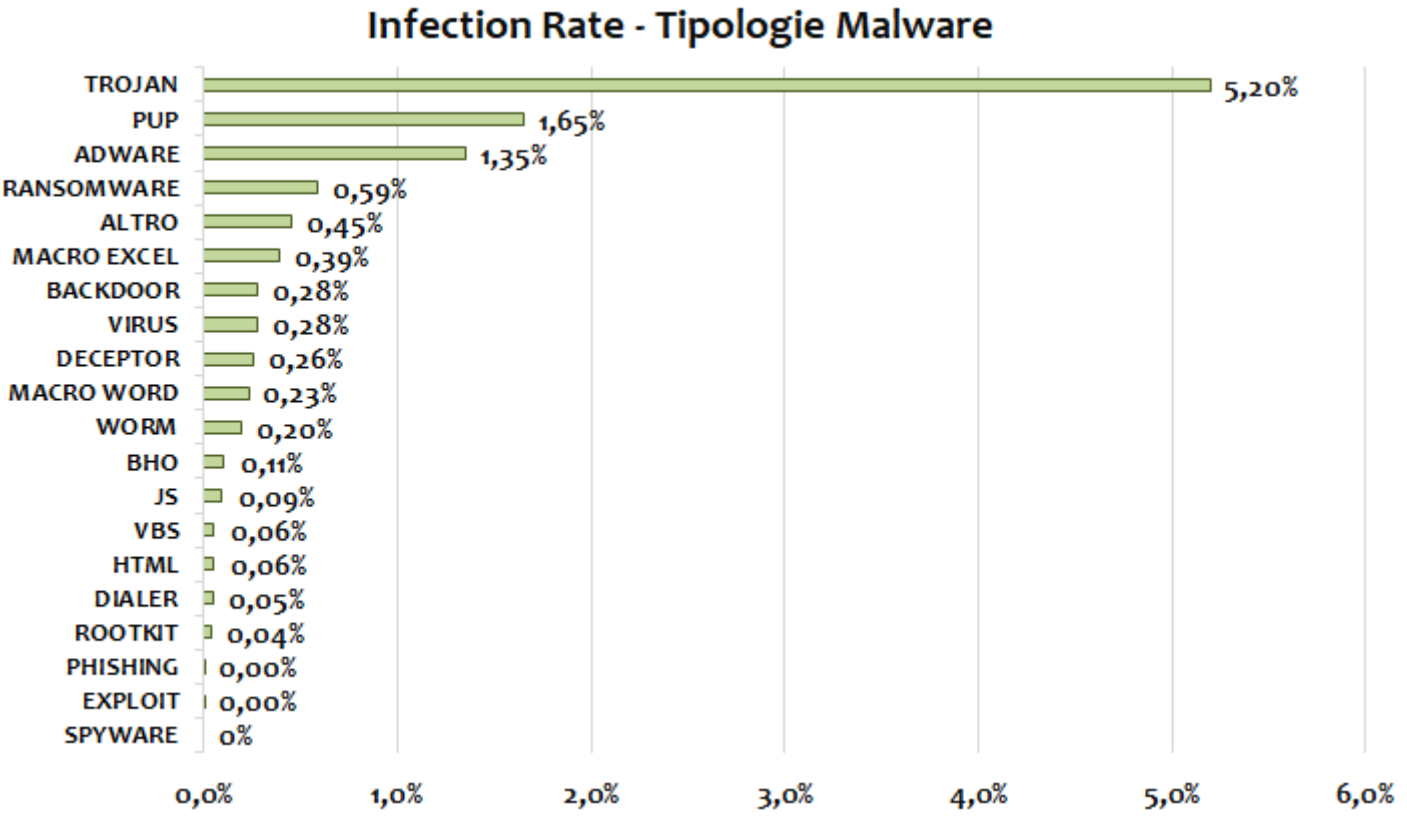
- Tipologia del malware
- Sistema operativo (client/server)

Al primo posto i **Trojan** con una percentuale del 5,20%. Secondo posto confermato per i **PUP** , con una percentuale dell'1,65%. Terzo gradino del podio per la categoria **Adware** con l'1,35%.

Salgono in quarta posizione i **Ransomware** con lo 0,59%. 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.).

Il gruppo generico denominato **Altro** (che include le macro di Office generiche) si posizionano al quinto posto con il 0,45%.



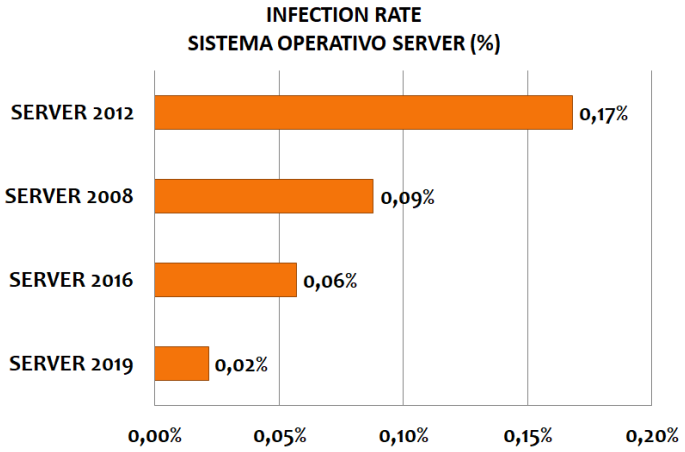
Andiamo ora ad analizzare la prevalenza delle infezioni del mese di giugno in base ai sistemi operativi suddivisi tra sistemi Server e Client.

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 (0,17%) seguito da Windows Server 2008 (0,09%),

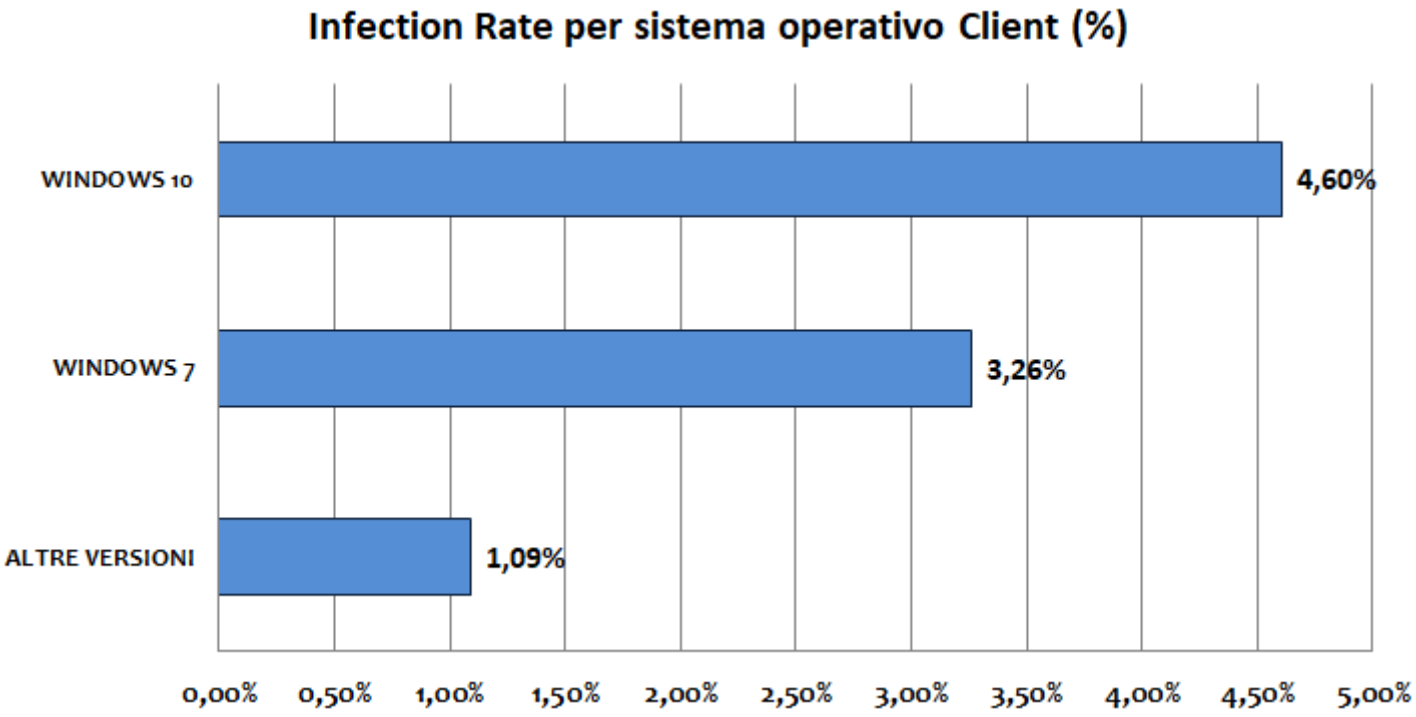
Windows Server 2016 si attesta terzo posto con lo 0,06%. Chiude Windows Server 2019 con lo 0,02%.

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 giugno abbiamo riscontrato che circa l'**8,95%** dei terminali è stato infettato o ha subito un attacco. Questo dato indica che **1 computer su 11** è stato colpito da malware nel mese di giugno.

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

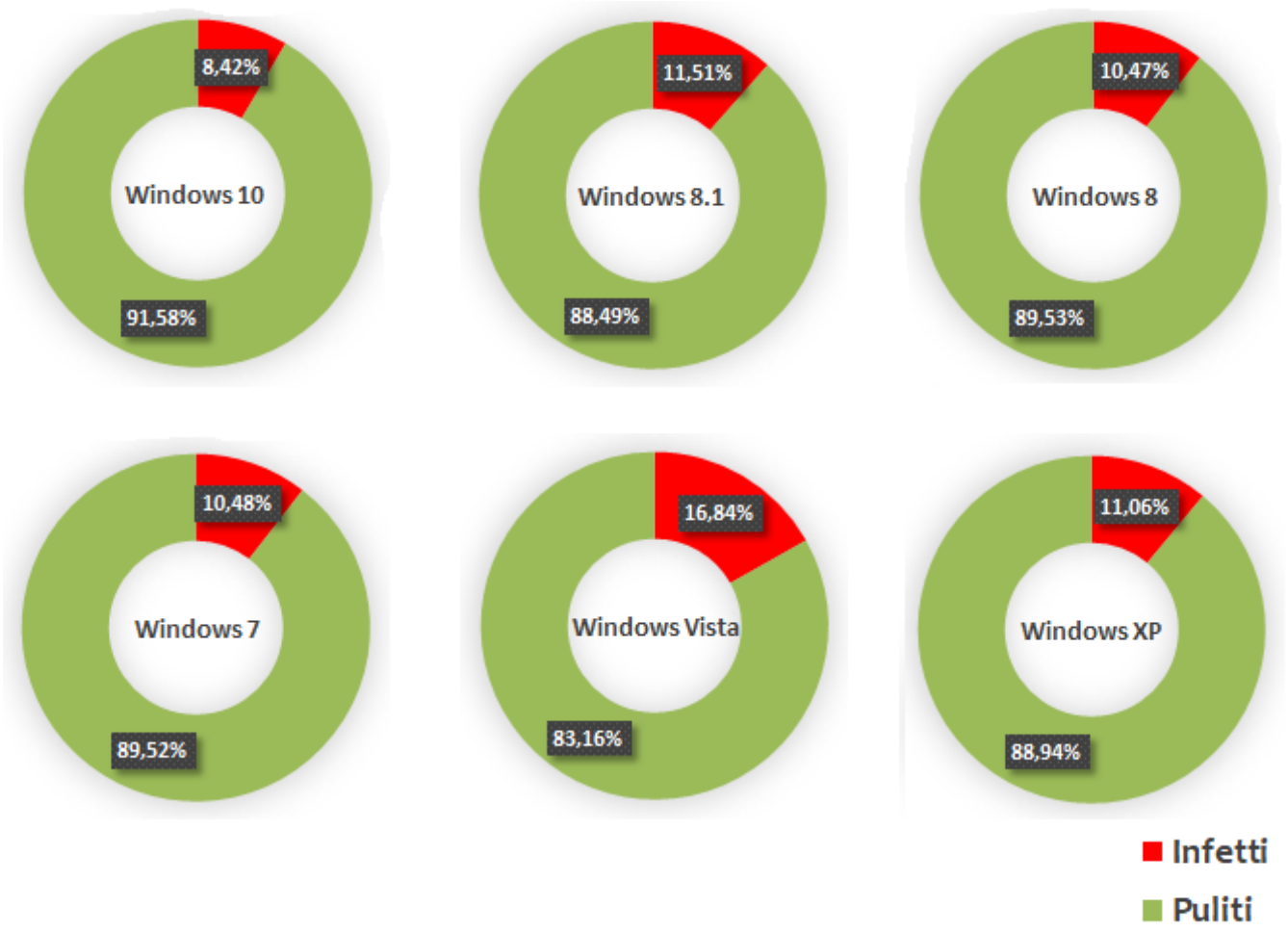


Windows 10 e **Windows 7** coprono quasi l'88% del parco macchine dei Client, pertanto gli altri sistemi operativi sono stati raccolti in un unico gruppo.

Nel grafico della pagina precedente, relativo ai Client, prima posizione per **Windows 10** con il 4,60%. Secondo **Windows 7** il 3,26%. Gli altri sistemi operativi si attestano appena sopra al punto percentuale ovvero all'1,09%.

Ma quale sarà il sistema operativo più sicuro ?

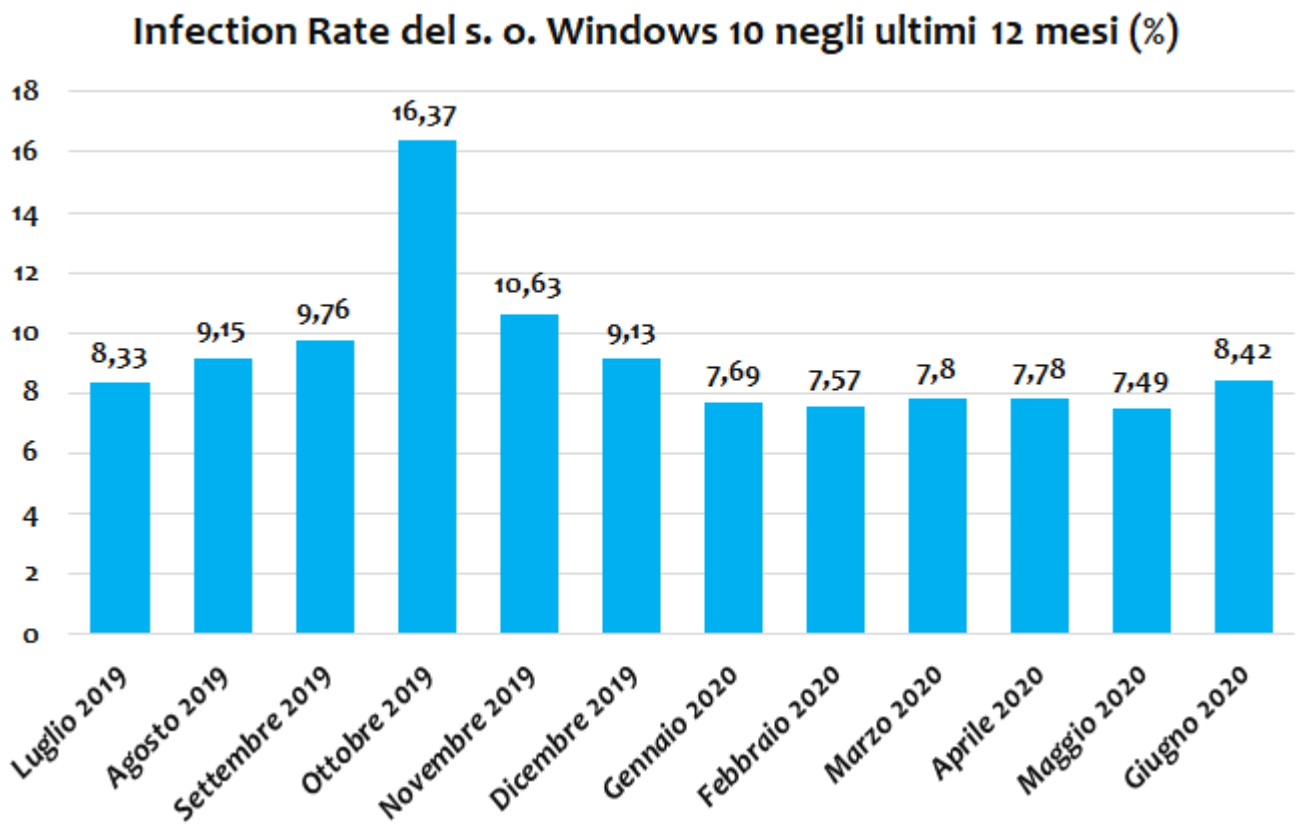
Per rispondere a questa domanda dobbiamo calcolare la prevalenza d'infezione sul medesimo sistema operativo. Prendendo ad esempio Windows 10, si può notare che il rate di infezione tra tutte le macchine ove è installato Windows 10 che ha subito un attacco informatico è dell'8,42% . Con questo calcolo possiamo capire quindi qual è il sistema operativo più sicuro.



Nei grafici a torta è stato calcolato l'Infection Rate (IR) relativo alla prevalenza sul medesimo sistema operativo client. Il sistema operativo che ha subito meno attacchi risulta essere Windows 10, questo dimostra che utilizzare sistemi operativi moderni e supportati riduce il rischio di infezione. I sistemi operativi non più supportati da Microsoft, come Windows XP e Vista, hanno di fatto il rate d'infezione molto più alto. Paragonando Windows Vista a Windows 10, si può notare infatti che l'IR è 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 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. Nel mese di giugno registriamo un aumento delle infezioni rispetto ai primi 5 mesi del 2020.



TG Soft
Cyber Security Specialist
www.tgsoft.it