Analisi di un Cyber Attacco sofisticato

Author : Giuseppe Brando

Date : 9 Aprile 2019

Questo articolo vuole essere un modo per avvicinare il lettore a comprendere la complessità degli attacchi cyber. Di seguito verrà trattato un *modus operandi* molto particolare con un focus specifico sulla grafica, sulle operazioni bit a bit[1] (AND, NOT, OR, XOR) e, quindi, con un pizzico di matematica.

Le operazioni bit a bit sono operazioni primitive e veloci, tant'è che spesso sono implementate nei processori a basse prestazioni perché più veloci da svolgere rispetto alle classiche operazioni aritmetiche (divisione, moltiplicazione, somma).

Partiremo dall'articolo pubblicato dalla società "360 Enterprise Security Group" e nello specifico dal suo team d'intelligence "360 Threat Intelligence Center" riguardante la vulnerabilità di WinRar (CVE-2018-20250)[2], resa nota il 2 febbraio di quest'anno, per poi vedere l'uso della stessa in attacchi cyber strutturati. In fine il lettore verrà condotto passo passo in un'analisi della Backdoor "Fileless[3]" che rappresenta, a mio parere, la parte più interessante per comprendere meglio la complessità degli attacchi cyber strutturati.

L'articolo, intitolato ***Warning! Upgrades in WinRAR Exploit with Social Engineering and Encryption***[4] riassume gli attacchi e le tecniche di social engineering orbitanti intorno a tale vulnerabilità. Questo riporta, come vettore iniziale di attacco, email di phishing che usano come pretesto opportunità lavorative in Arabia Saudita con l'obiettivo di convincere l'utente ad estrarre il file compresso e quindi avviare la compromissione.

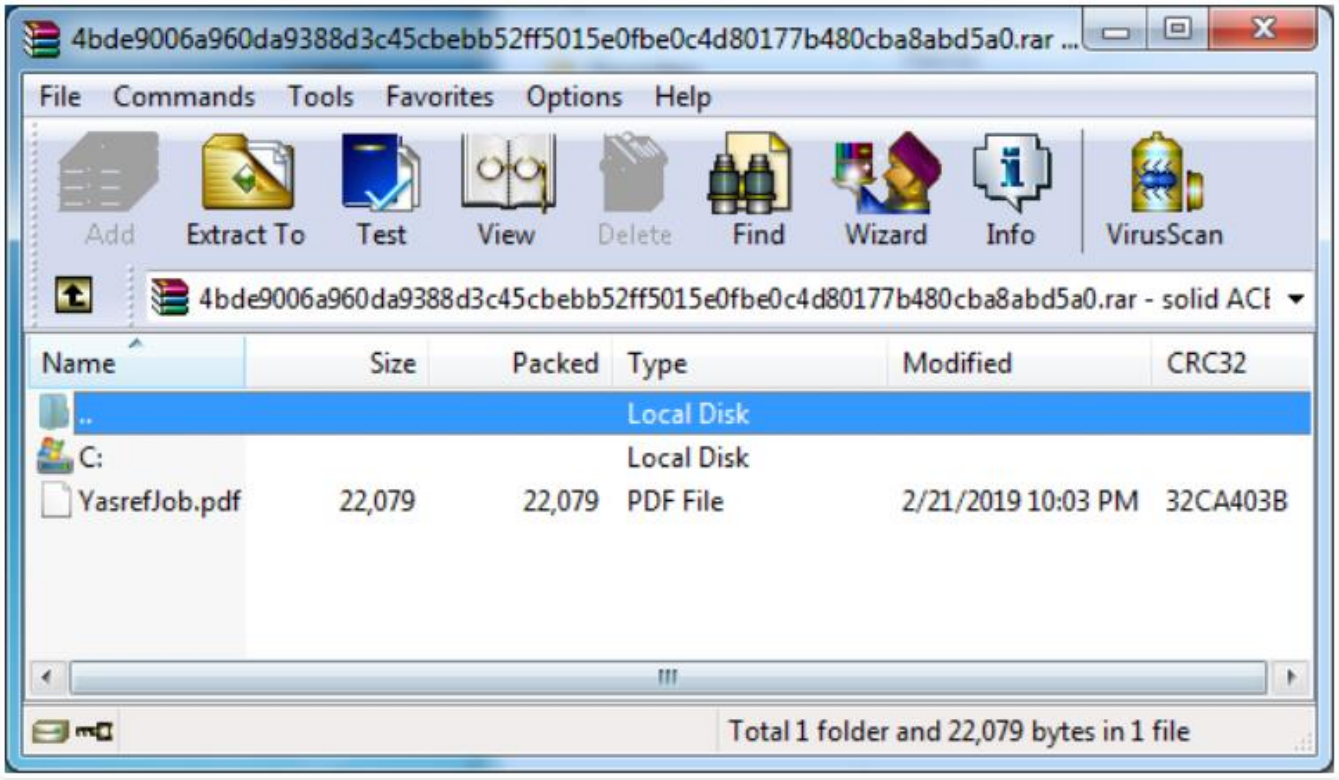
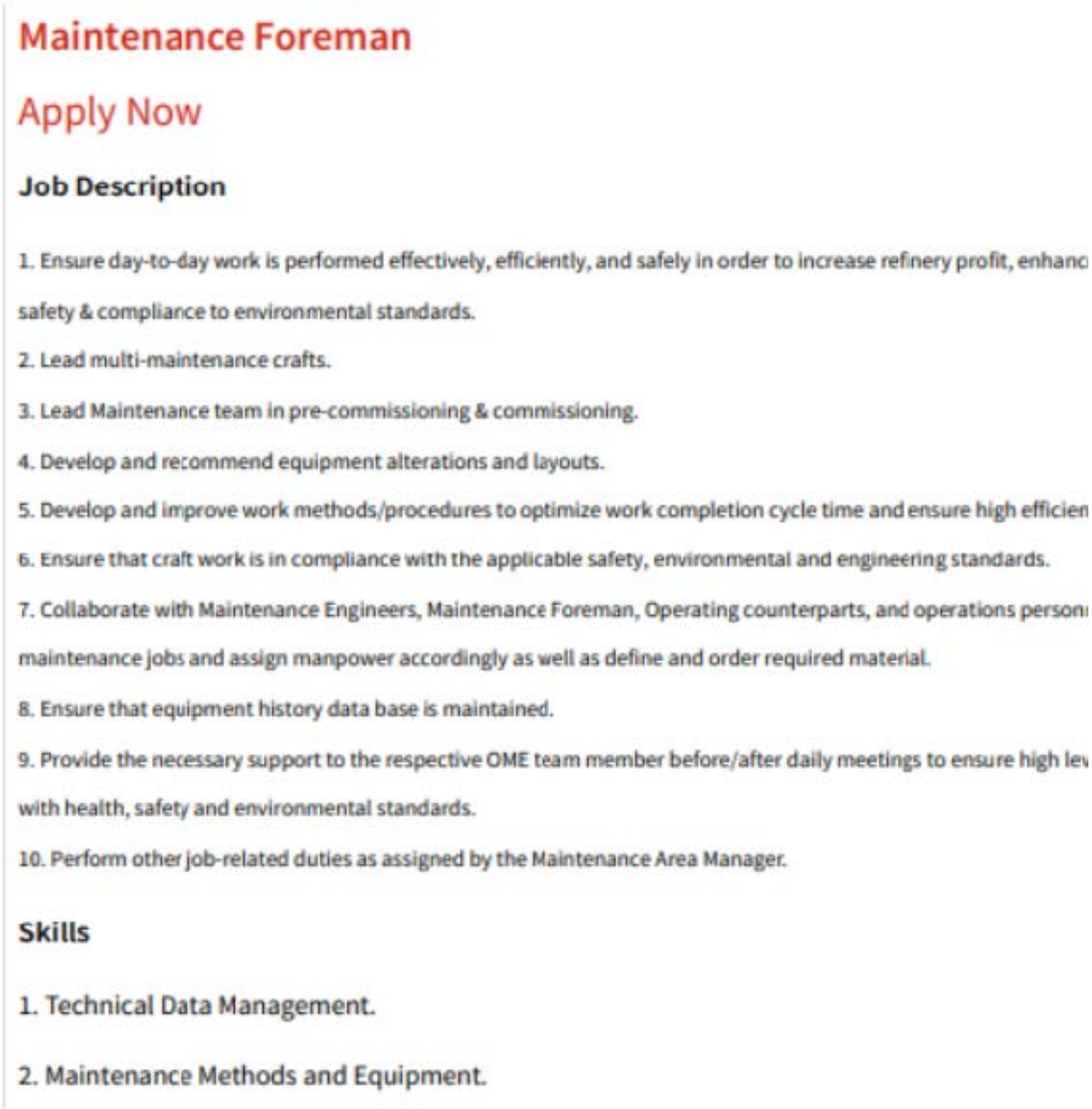


Immagine dell’archivio rar

A tale scopo, all’interno del file compresso è stato inserito un file PDF con una proposta di lavoro fittizia associata alla società “**YASREF**” - **Yanbu Aramco Sinopec Refining**, una una joint venture tra Saudi Aramco e China Petrochemical Corporation (Sinopec)[5].



Maintenance Foreman

Apply Now

Job Description

1. Ensure day-to-day work is performed effectively, efficiently, and safely in order to increase refinery profit, enhanc
safety & compliance to environmental standards.
2. Lead multi-maintenance crafts.
3. Lead Maintenance team in pre-commissioning & commissioning.
4. Develop and recommend equipment alterations and layouts.
5. Develop and improve work methods/procedures to optimize work completion cycle time and ensure high efficien
6. Ensure that craft work is in compliance with the applicable safety, environmental and engineering standards.
7. Collaborate with Maintenance Engineers, Maintenance Foreman, Operating counterparts, and operations person
maintenance jobs and assign manpower accordingly as well as define and order required material.
8. Ensure that equipment history data base is maintained.
9. Provide the necessary support to the respective OME team member before/after daily meetings to ensure high lev
with health, safety and environmental standards.
10. Perform other job-related duties as assigned by the Maintenance Area Manager.

Skills

1. Technical Data Management.
2. Maintenance Methods and Equipment.

Immagine del PDF contenuto all’interno dell’archivio Rar

Il primo fatto degno di nota è che il PDF in sé non contiene nessun componente malevolo: la vulnerabilità di WinRar provvede all’infezione della macchina appena l’archivio viene decompresso.

Tralasciando tutti i tecnicismi di come viene sfruttata tale vulnerabilità e di come, quindi, l’infezione sia avvenuta (per questi dettagli si rimanda all’articolo originale), è utile per il lettore notare che alla fine della prima fase del processo di compromissione verrà “letta” una specifica immagine remota.

La parola “letta” è posta appositamente tra apici per far notare al lettore che l’immagine non

viene scaricata ma, come già detto, letta da remoto (attacco fileless).

Arrivati a questo punto siamo nella parte più interessante dell'attacco. L'immagine in questione, sotto riportata, è un semplice paesaggio montano, in formato PNG, con una dimensione di 300x300 pixel.

Da notare che l'immagine di per sé, senza uno specifico script che ne interpreti il contenuto, non rappresenta una componente malevola.

Immagine usata per nascondere il codice malevolo

A questo punto sorgerà spontanea, nel lettore, la curiosità di capire come sia possibile che la successiva fase della compromissione abbia come fonte questa immagine.

L'attaccante è stato molto abile e astuto in questo attacco. Partendo dall'immagine e sfruttando solamente i primi 3000 pixel (anche se, in realtà, i pixel usati sono stati per la precisione 2864), ha "giocato" con i colori variandone la gradazione in modo da poter estrarre da ogni pixel un carattere. Quanto detto è stato fatto usando una specifica formula che vedremo successivamente.

Per essere più chiari nell'illustrare la tecnica utilizzata, bisogna innanzitutto dire che un pixel è formato dai 3 colori base (Rosso, Verde, Blu) più il colore Alpha, che indica l'opacità/trasparenza. Ogni colore può avere una gradazione che va da 0 a 255, interpolando i valori dei tre colori principali il pixel assume uno specifico colore. Nell'immagine sottostante possiamo vedere come questi valori vengono interpretati dai computer e per maggiore

chiarezza utilizziamo come esempio i valori del colore “GreenYellow”.

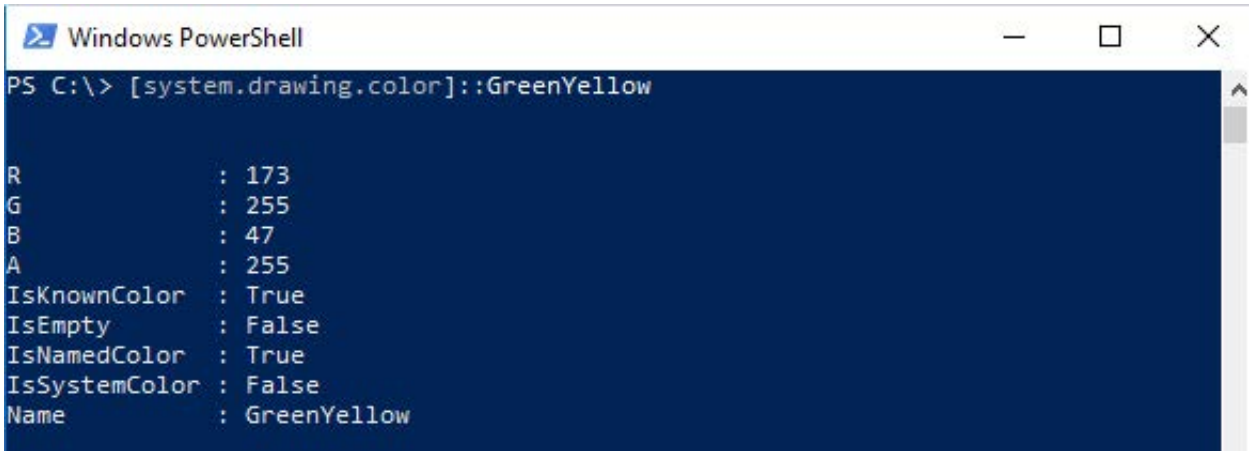


Immagine che illustra come il computer interpreta i colori

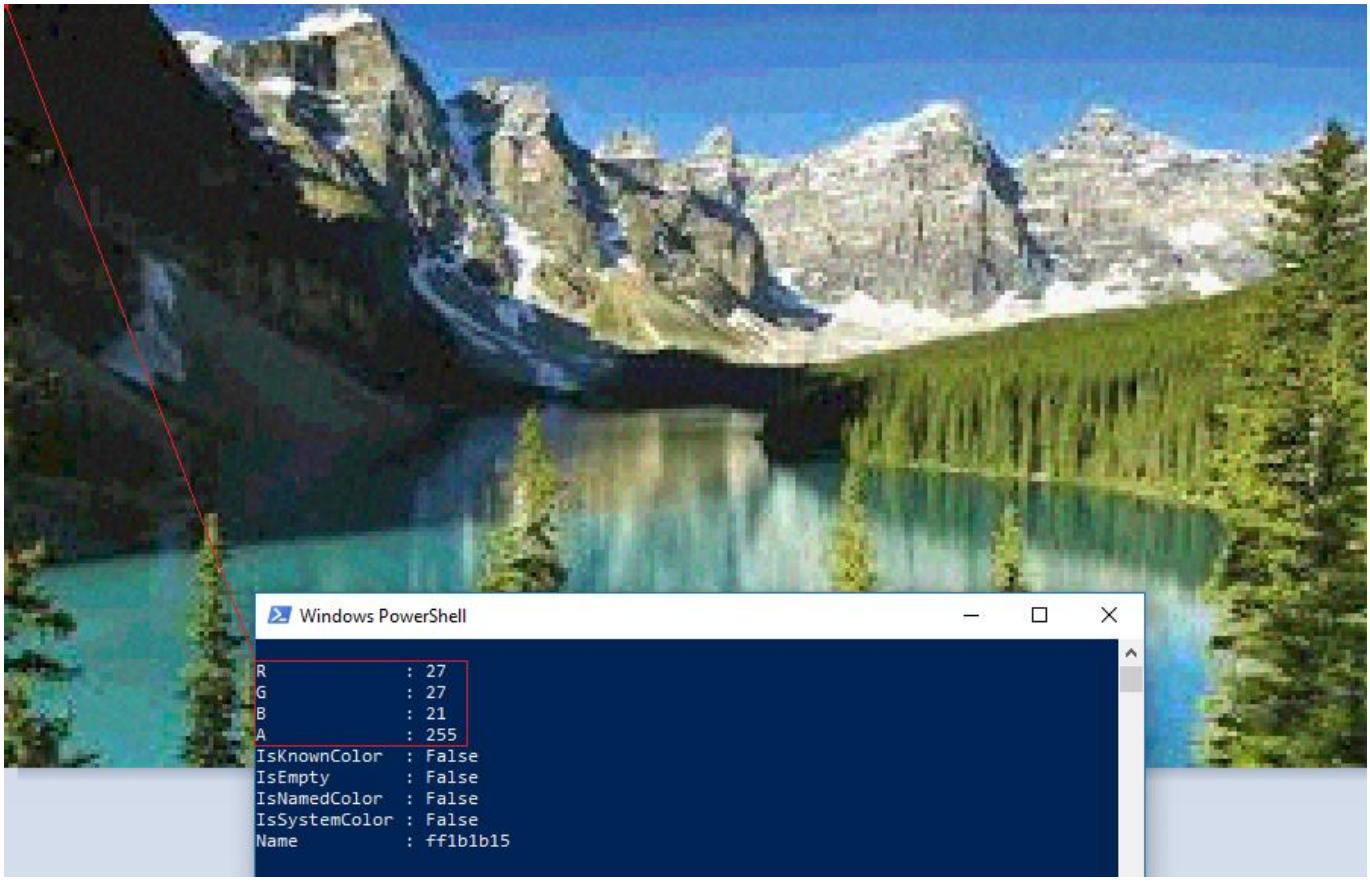
L’attaccante pertanto ha modificato leggermente la gradazione dei primi 3.000 pixel (una matrice di 10 righe per 300 colonne) e nello specifico la gradazione del colore Blu e il verde, molto predominanti in quell’area dell’immagine (racchiusa nel rettangolo rosso) rendendo, pertanto, quasi impossibile percepire la modifica a occhio nudo.

Immagine che illustra l’area dove è nascosto il codice malevolo da estrarre

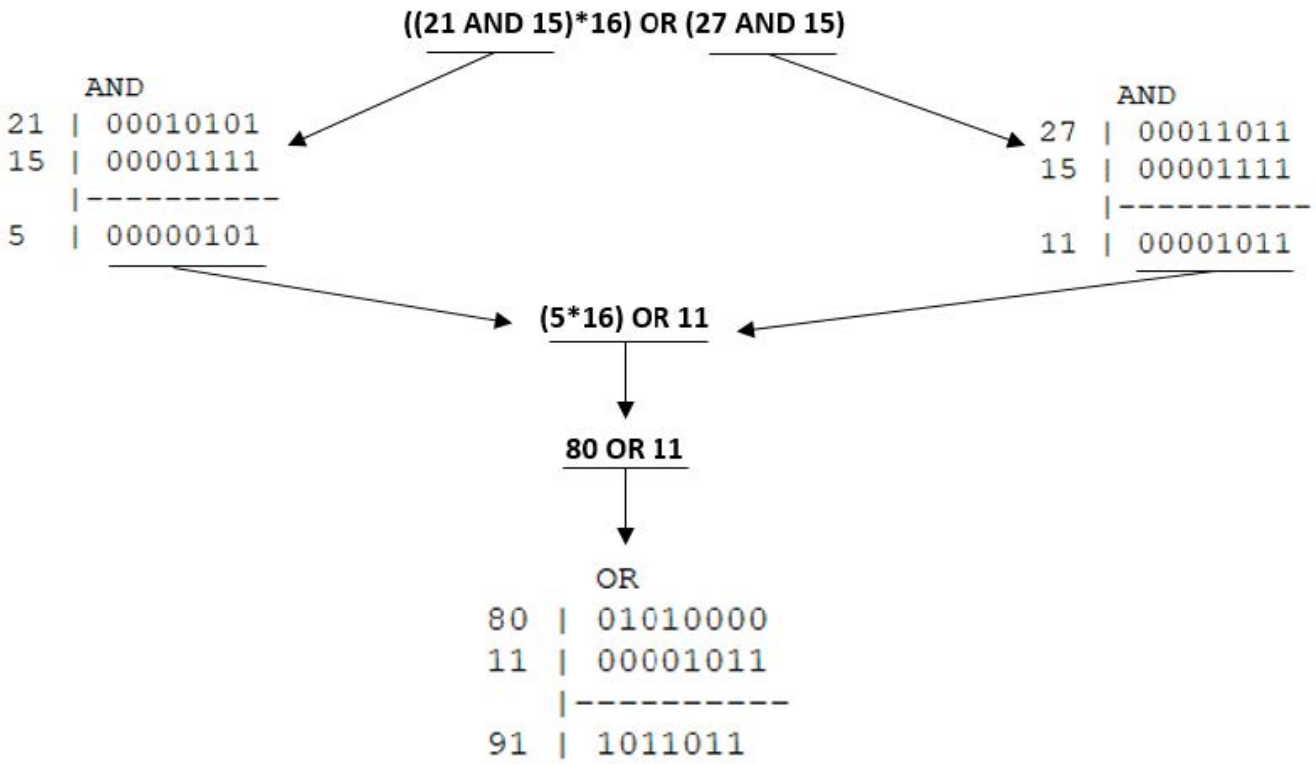
Grazie ad approfondite conoscenze di grafica, all’attaccante è bastato mettere a punto una specifica formula logico/matematica per riuscire a estrarre il carattere desiderato da ogni pixel e quindi costruire lo script da eseguire (tecnica stenografica).

La formula usata è la seguente:

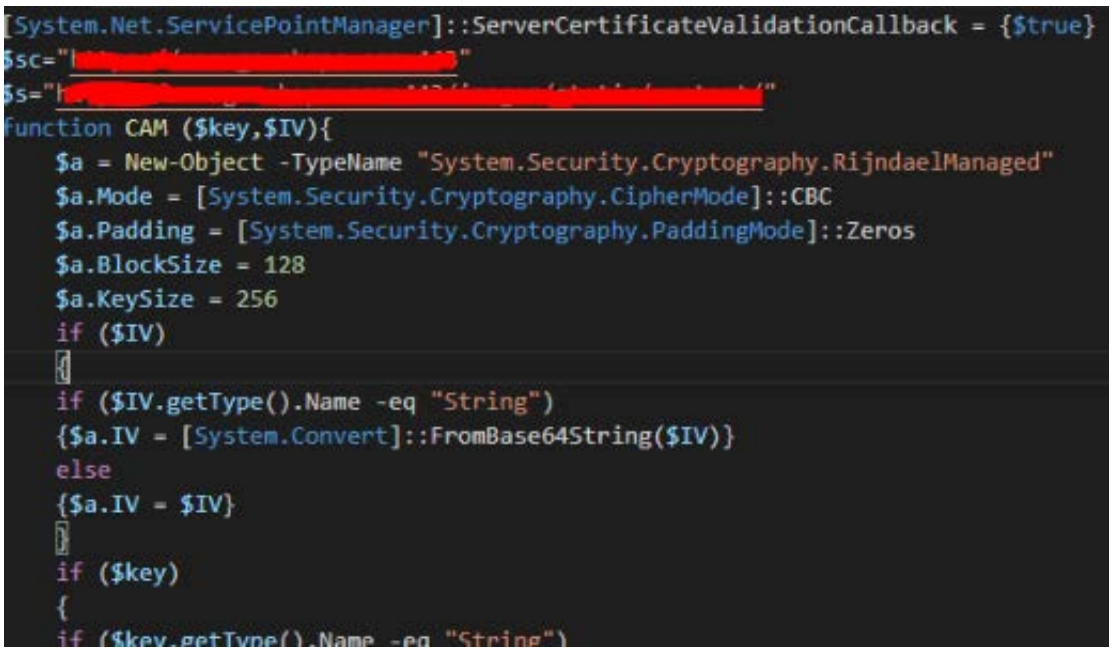
((Valore_Colore_Pixel _Blue AND 15)*16) OR (Valore_Colore_Pixel_Verde AND 15)



Data l’immagine e i valori del primo pixel (Blu:21, Verde:27, Rosso:27, Alpha:255), tenendo in considerazione il valore del colore blue e del colore verde, la formula si trasforma come segue:



Infine, il numero **91** (risultato di tutta l'operazione) viene trasformato in un carattere ASCII[6], in questo caso otteniamo il carattere di parentesi quadra aperta "**[**". Di seguito un estratto dello script nascosto dentro l'immagine.



```
[System.Net.ServicePointManager]::ServerCertificateValidationCallback = {$true}
$sc="[redacted]"
$s="[redacted]"
function CAM ($key,$IV){
    $a = New-Object -TypeName "System.Security.Cryptography.RijndaelManaged"
    $a.Mode = [System.Security.Cryptography.CipherMode]::CBC
    $a.Padding = [System.Security.Cryptography.PaddingMode]::Zeros
    $a.BlockSize = 128
    $a.KeySize = 256
    if ($IV)
    {
    if ($IV.getType().Name -eq "String")
    {$a.IV = [System.Convert]::FromBase64String($IV)}
    else
    {$a.IV = $IV}
    }
    if ($key)
    {
    if ($key.getType().Name -eq "String")
```

Come è facile intuire, si tratta di un attacco molto strutturato che fa leva su diverse componenti:

- tecniche di Social Engineering (opportunità lavorative e nomi di società importanti nel settore energetico e oil & gas);
- malware di tipo Fileless;
- nuove vulnerabilità, in questo caso scoperta pochi giorni prima;
- tecniche di stenografia per nascondere informazioni all'interno delle immagini.

Quanto appreso da questo articolo deve costituire un **monito per il lettore** a non sottovalutare le minacce nel mondo cyber. Un modo per intuire che anche un'immagine banale, o all'apparenza tale, può nascondere al suo interno una minaccia ben più critica di quando si possa immaginare. Specialmente gli attori strutturati e con elevate capacità, spesso sponsorizzati da uno Stato, hanno strumenti molto sofisticati che possono essere impiegati nelle diverse fasi di un attacco, per non parlare delle avanzate tecniche che sono in grado di mettere in atto durante ogni fase della compromissione

Note:

[1] https://it.wikipedia.org/wiki/Operazione_bit_a_bit

[2] https://nvd.nist.gov/vuln/detail/CVE-2018-20250

[3] https://en.wikipedia.org/wiki/Fileless_malware

[4] https://ti.360.net/blog/articles/upgrades-in-winrar-exploit-with-social-engineering-and-encryption/

[5] https://www.yasref.com/en-us/Pages/About.aspx

[6] https://it.wikipedia.org/wiki/ASCII

Articolo a cura di **Giuseppe Brando**