

# Report Esercizio

W20-D3



---

**Redatto da Andrea Sciattella**

03/07/2024

## TRACCIA

---

Lavoriamo in un'azienda in un SOC o CSIRT in una grande azienda e due utenti segnalano problemi sui loro computer e chiedono assistenza al reparto tecnico (che siamo noi)

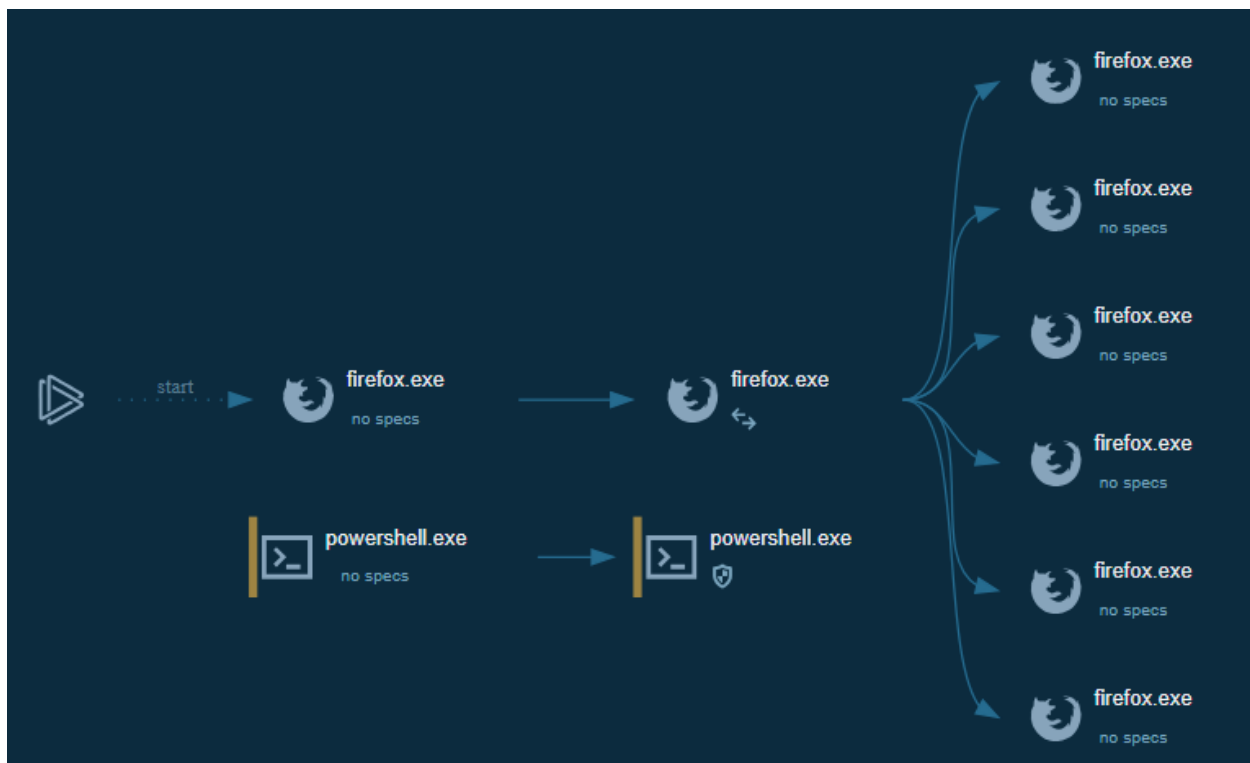
Analizzare i seguenti link e fare un **piccolo report** di quello che si scopre relativo alla segnalazione dell'eventuale attacco.

<https://tinyurl.com/linklosco1> e <https://tinyurl.com/linklosco2>

## SVOLGIMENTO ESERCIZIO N.1

Analizziamo attentamente l'istanza su "any.run", dagli alert della webapp vengono descritti problemi come **"Bypass execution policy to execute commands, Using PowerShell to operate with local accounts, Reads the Internet Settings, the process bypasses the loading of PowerShell profile settings"**.

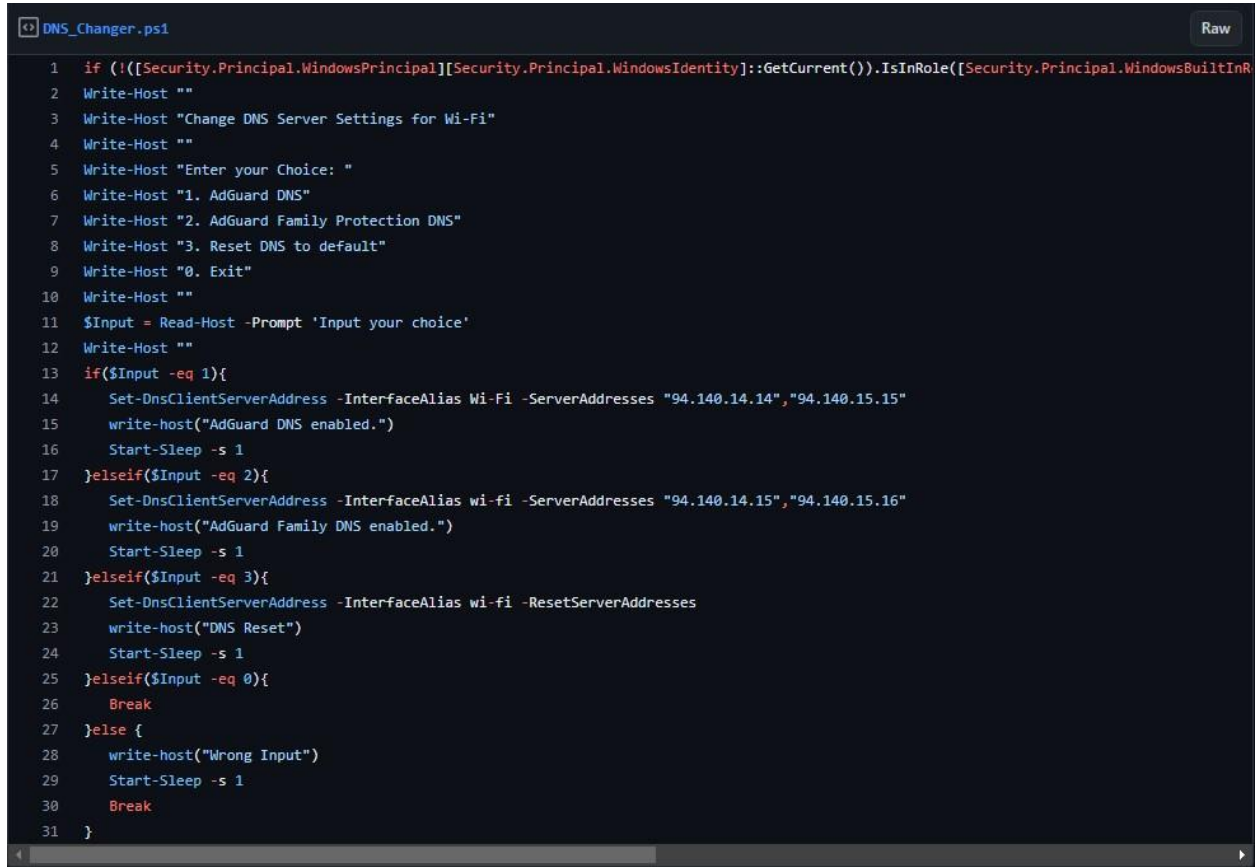
Controlliamo passo per passo tutti gli step compiuti durante l'istanza per verificare se si tratta di un vero attacco o no.



(Grafico sviluppato dalla piattaforma any.run che mette in evidenza tutti processi della macchina, compresi quelli potenzialmente dannosi.)

Dal grafico notiamo immediatamente due processi aperti in powershell.exe che potrebbero crearci problemi.

- Dal n.1 al n.8 screenshot, possiamo vedere l'utente navigare sul browser Mozilla verso il sito "gist.github", una piattaforma fornita da GitHub che permette agli utenti di condividere frammenti di codice e altro. Solitamente sicuro, si consiglia di revisionare il codice da voler usare per assicurarsi di non aver scaricato un malware.

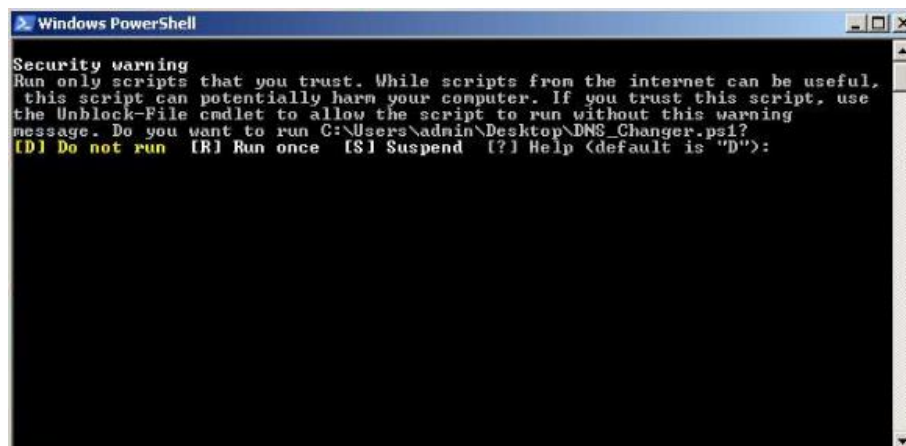


```

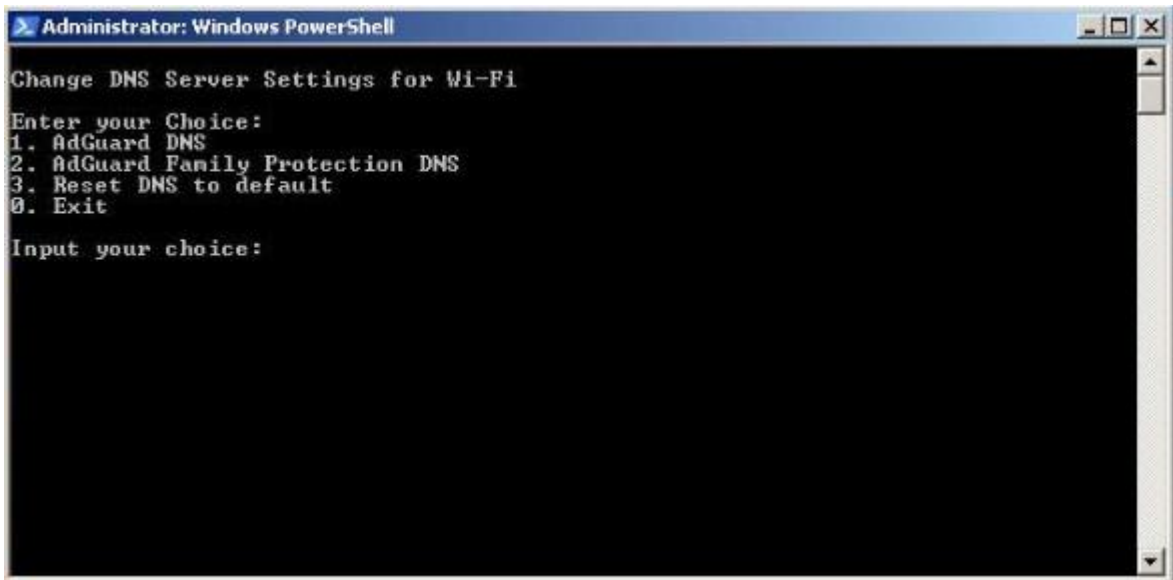
1  if (!(Security.Principal.WindowsPrincipal)[Security.Principal.WindowsIdentity]::GetCurrent().IsInRole([Security.Principal.WindowsBuiltInR
2  Write-Host ""
3  Write-Host "Change DNS Server Settings for Wi-Fi"
4  Write-Host ""
5  Write-Host "Enter your Choice: "
6  Write-Host "1. AdGuard DNS"
7  Write-Host "2. AdGuard Family Protection DNS"
8  Write-Host "3. Reset DNS to default"
9  Write-Host "0. Exit"
10 Write-Host ""
11 $Input = Read-Host -Prompt 'Input your choice'
12 Write-Host ""
13 if($Input -eq 1){
14     Set-DnsClientServerAddress -InterfaceAlias Wi-Fi -ServerAddresses "94.140.14.14","94.140.15.15"
15     write-host("AdGuard DNS enabled.")
16     Start-Sleep -s 1
17 }elseif($Input -eq 2){
18     Set-DnsClientServerAddress -InterfaceAlias wi-fi -ServerAddresses "94.140.14.15","94.140.15.16"
19     write-host("AdGuard Family DNS enabled.")
20     Start-Sleep -s 1
21 }elseif($Input -eq 3){
22     Set-DnsClientServerAddress -InterfaceAlias wi-fi -ResetServerAddresses
23     write-host("DNS Reset")
24     Start-Sleep -s 1
25 }elseif($Input -eq 0){
26     Break
27 }else {
28     write-host("Wrong Input")
29     Start-Sleep -s 1
30     Break
31 }

```

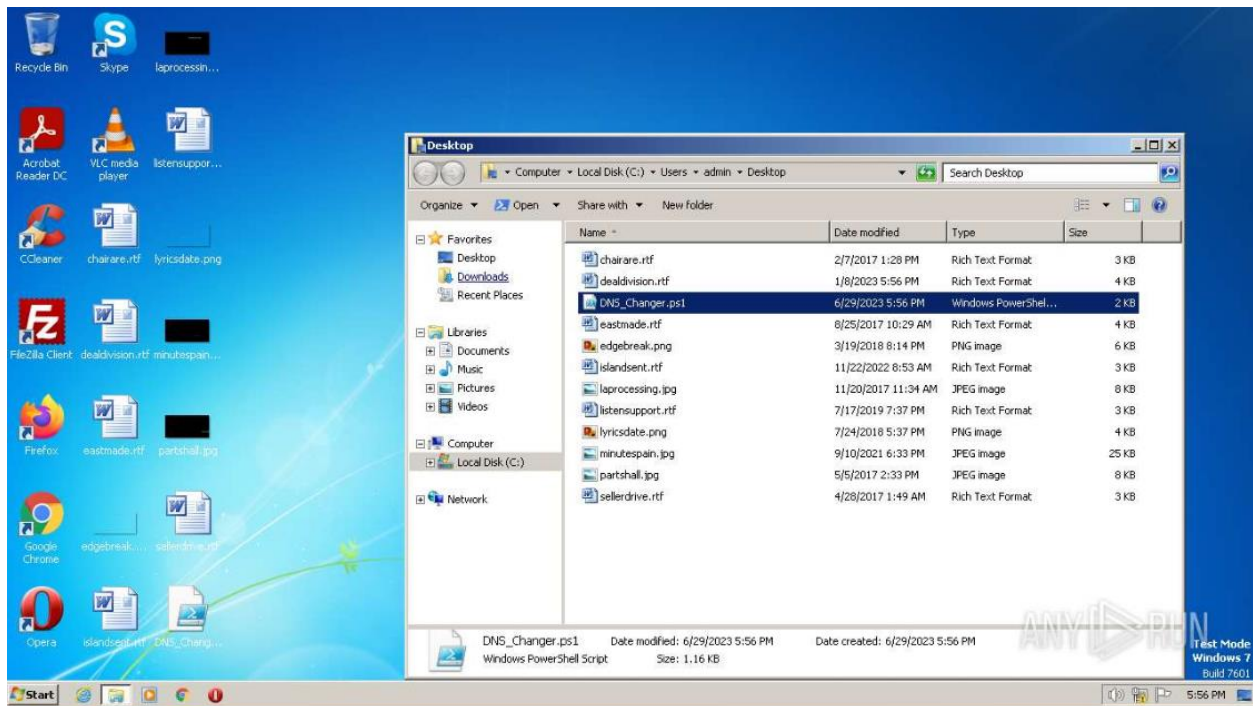
- Successivamente viene scaricato lo script, e nonostante i diversi avvisi viene eseguito lo stesso.



- Una volta runnato lo script vengo stampate a schermo delle opzioni per la modifica del DNS della macchina attraverso i DNS di AdGuard e viene scelta una delle opzioni (1 o 2).



- Durante l'esecuzione dello script sorgono dunque i problemi rilevati, creati esattamente da questo script di powershell.



- La riproduzione degli screenshot termina con lo screen dello script (DNS\_Changer.ps1) salvato nel disco locale.

## CONCLUSIONI ESERCIZIO N.1

---

In conclusione, dopo un'attenta analisi dell'istanza "ANY.RUN" che inizialmente indicava un potenziale attacco, il nostro approfondimento ha rivelato che si trattava di **uno script di cambio DNS** con gli stessi presenti sul sito ufficiale di **AdGuard** (sostanzialmente per **bloccare pubblicità e tracker**). Questo script, una volta eseguito, ha attivato un allarme su **ANY.RUN** per via delle modifiche repentine alle impostazioni di rete autorizzate da un semplice script, che ha contribuito a far emergere rapidamente il comportamento sospetto.

### Osservazioni Chiave:

1. **Natura dello Script:** Lo script esaminato al codice sorgente, è stato identificato come uno script di cambio DNS, il cui scopo era di modificare le impostazioni DNS del sistema per evitare pubblicità e tracker online.
2. **Allarme di ANY.RUN:** L'esecuzione dello script ha attivato un allarme su ANY.RUN, sottolineando l'efficacia della piattaforma nel rilevare comportamenti potenzialmente dannosi o non autorizzati.
3. **Impatto Potenziale:** Sebbene lo script non fosse dannoso di per sé, la modifica delle impostazioni DNS può avere gravi implicazioni, come il dirottamento del traffico internet, l'intercettazione dei dati e l'accesso a risorse non autorizzate nel caso di programma malevolo.