

Report Incident response W20D1

In questo esercizio dato uno scenario in cui un sistema azienda è stato compromesso, dovremo mostrare le tecniche di isolamento e rimozione del sistema infetto.

Sarà inoltre necessario fornire una definizione di clear, purge e destroy.

Isolamento:

Nella fase di isolamento il team CSIRT deve isolare la macchina infetta dal resto della rete, come prima azione immediata tramite EDR (endpoint detection and response), in modo che la macchina infetta sia in quarantena.

Questo però non isola la macchina infetta dal web.

Rimozione:

Successivamente sarà necessario scollegare la macchina dalla rete fisicamente in modo che l'attaccante non abbia più alcun modo per interagire con essa.

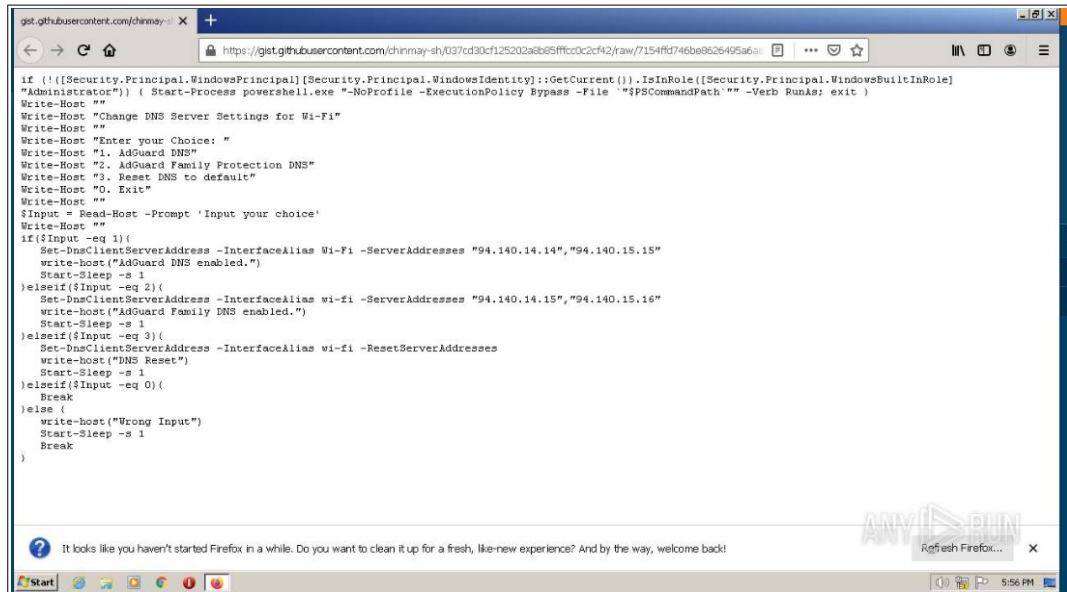
Metodo	Descrizione	Livello di sicurezza	Scopo finale
Clear	Rimozione superficiale: i dati vengono cancellati usando comandi standard. Non resiste a tecniche di recupero.	Basso	Reset rapido di sistemi poco critici
Purge	Sovrascrittura sicura o smagnetizzazione dei dischi. I dati sono resi irrecuperabili senza distruggere il supporto.	Medio/alto	Dati sensibili compromessi, ma si vuole riutilizzare l'hardware
Destroy	Distruzione fisica del supporto (triturazione, perforazione, incenerimento). Nessuna possibilità di recupero.	Alto	Dati classificati o altamente sensibili sono stati compromessi

Facoltativo

Primo scenario

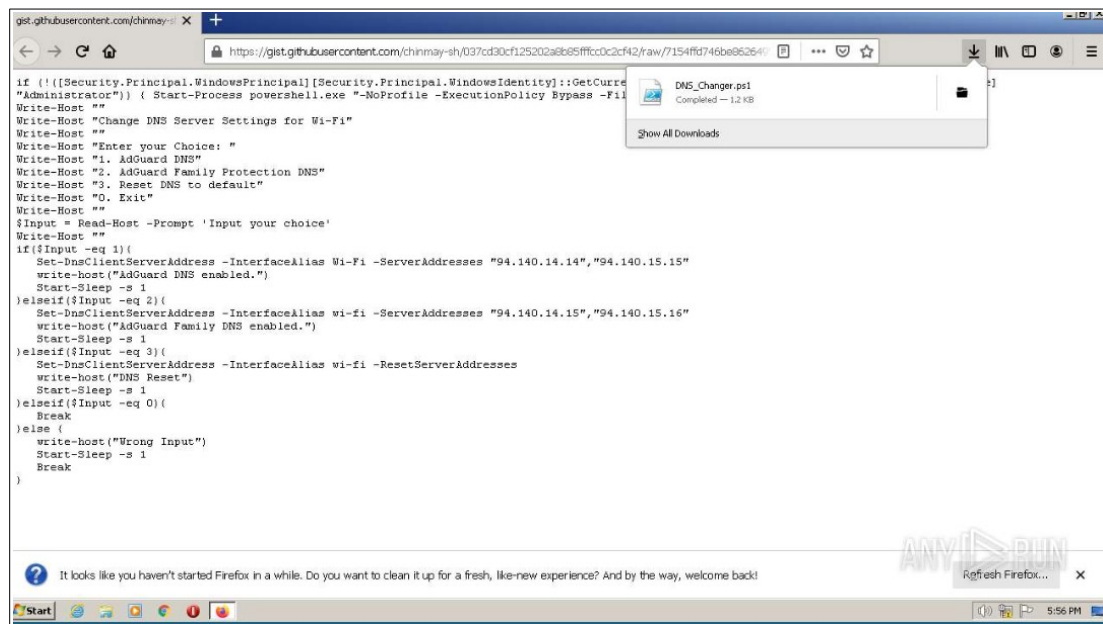
Un utente ha cliccato un link potenzialmente malevolo che lo ha indirizzato ad una pagina contenente uno script power shell.

Lo script consente all'utente di scegliere tra più opzioni per configurare o resettare i server DNS della scheda Wi-Fi, lo script non è esplicitamente malevolo ma in ambienti aziendali potrebbe far scattare degli alert di sicurezza.

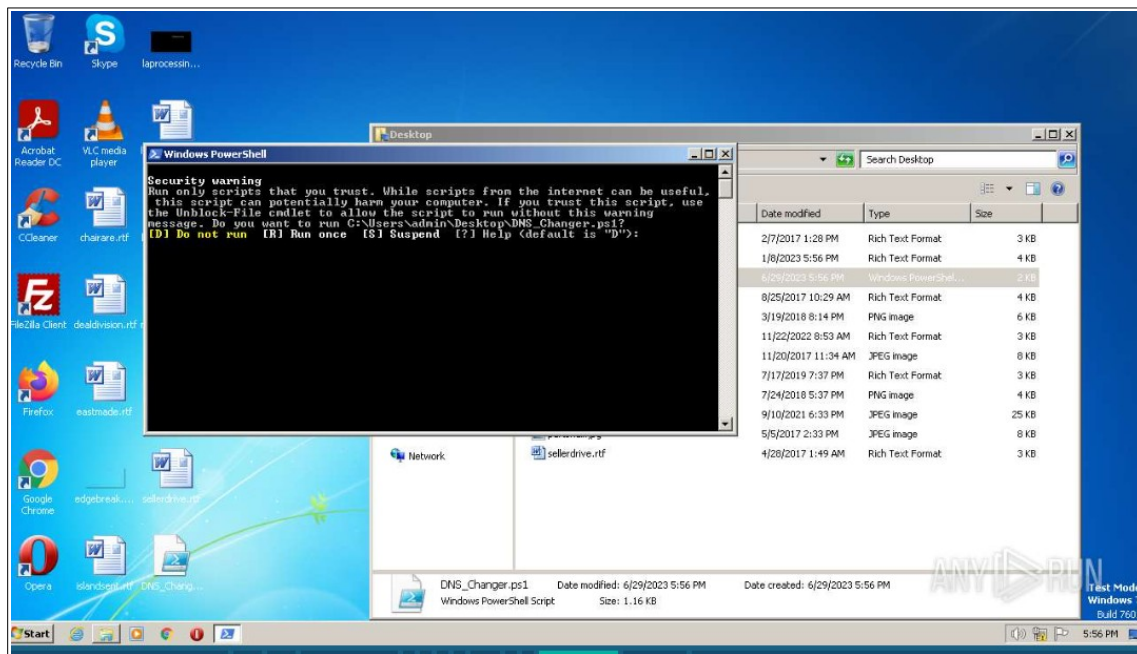


```
if ([Security.Principal.WindowsPrincipal][Security.Principal.WindowsIdentity]::GetCurrent()).IsInRole([Security.Principal.WindowsBuiltInRole]
"Administrator") { ( Start-Process powershell.exe "-NoProfile -ExecutionPolicy Bypass -File ""$PSCommandPath"" -Verb RunAs; exit )
Write-Host ""
Write-Host "Change DNS Server Settings for Wi-Fi"
Write-Host ""
Write-Host "Enter your Choice: "
Write-Host "1. AdGuard DNS"
Write-Host "2. AdGuard Family Protection DNS"
Write-Host "3. Reset DNS to default"
Write-Host "0. Exit"
Write-Host ""
$Input = Read-Host -Prompt 'Input your choice'
Write-Host ""
if($Input -eq 1){
    Set-DnsClientServerAddress -InterfaceAlias Wi-Fi -ServerAddresses "94.140.14.14","94.140.15.15"
    write-host("AdGuard DNS enabled.")
    Start-Sleep -s 1
}
elseif($Input -eq 2){
    Set-DnsClientServerAddress -InterfaceAlias wi-fi -ServerAddresses "94.140.14.15","94.140.15.16"
    write-host("AdGuard Family DNS enabled.")
    Start-Sleep -s 1
}
elseif($Input -eq 3){
    Set-DnsClientServerAddress -InterfaceAlias wi-fi -ResetServerAddresses
    write-host("DNS Reset")
    Start-Sleep -s 1
}
elseif($Input -eq 0){
    Break
}
else {
    write-host("Wrong Input")
    Start-Sleep -s 1
    Break
}
}
```

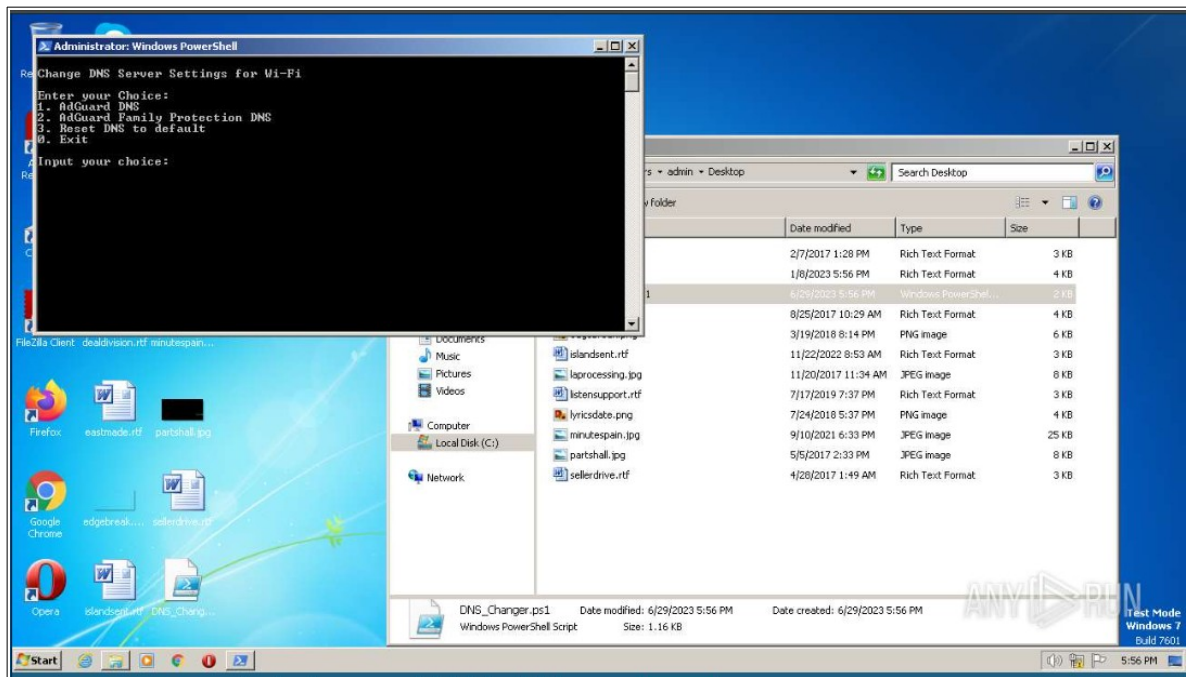
L'utente procede a salvare il file sul proprio PC.



Successivamente lo script viene eseguito e Power Shell invia un messaggio di sicurezza.

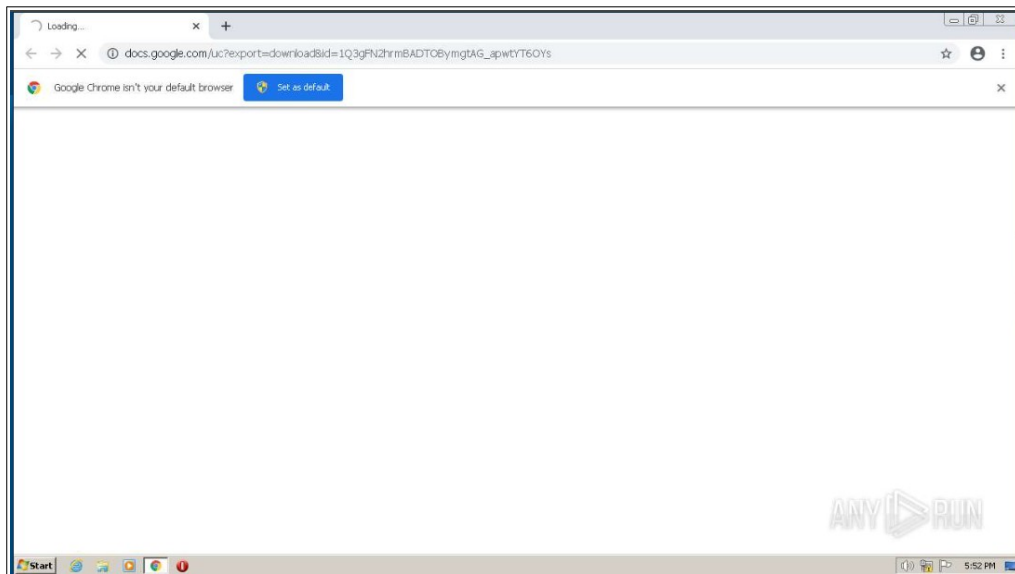


L'utente ignora l'avvertimento e si ritrova nel menù dello script.
È probabile che l'utente non abbia selezionato nessuna opzione in quanto ha successivamente chiuso Power Shell.

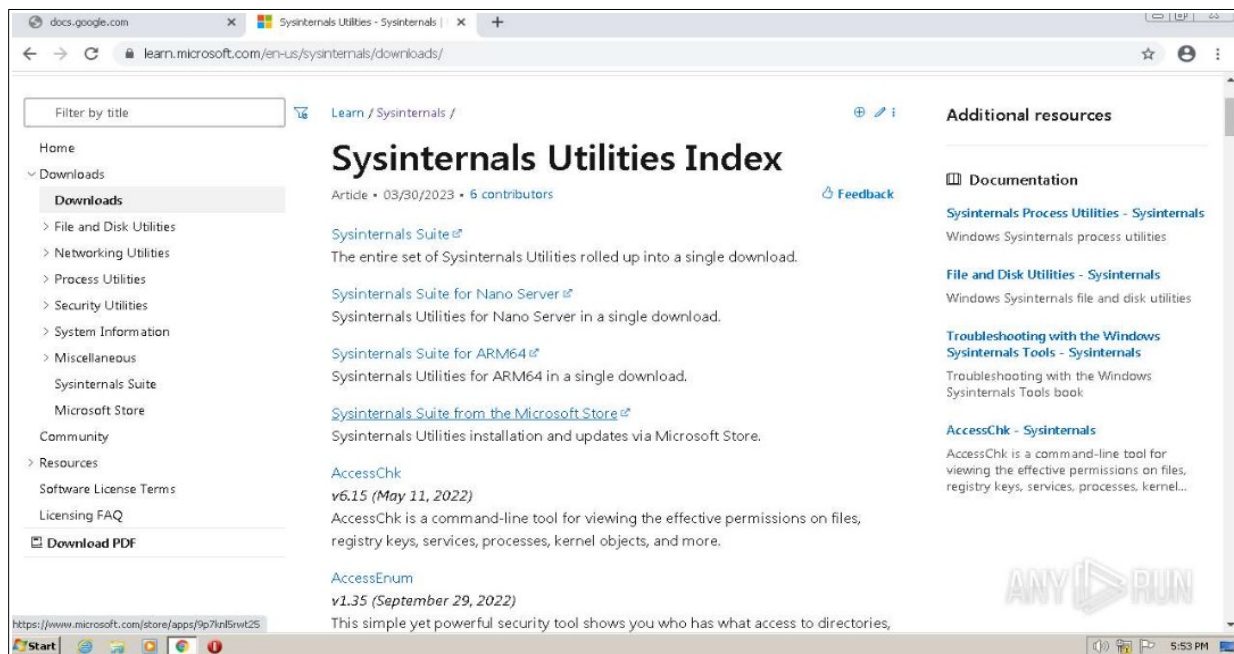


Secondo scenario

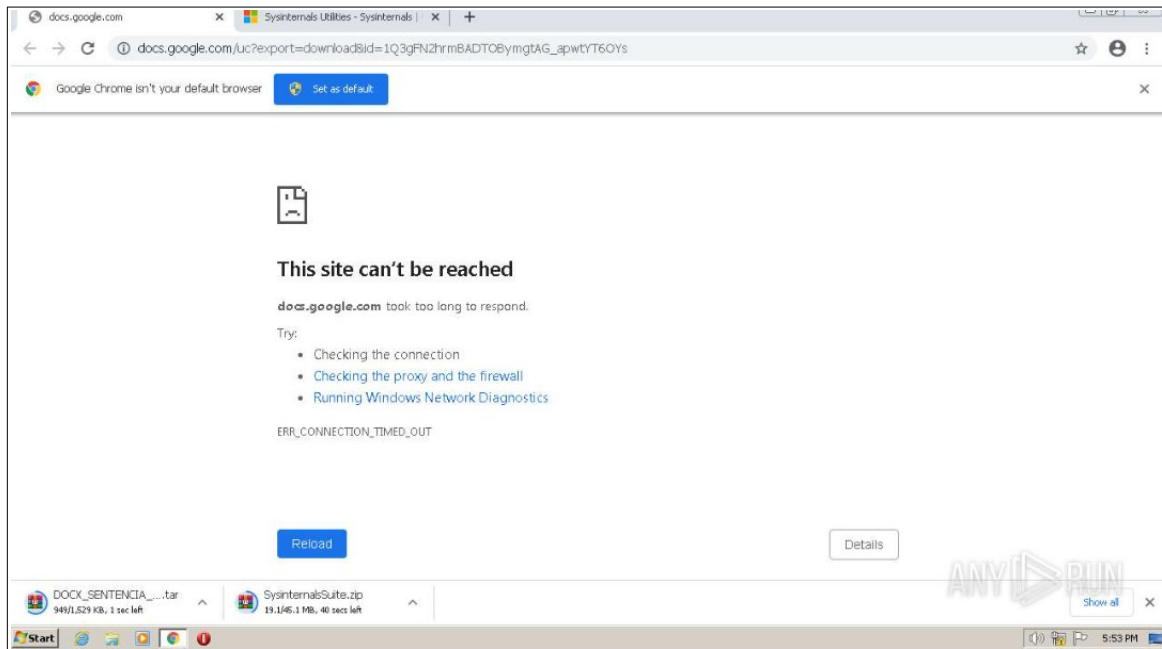
L'utente ha cliccato su un link potenzialmente malevolo ed è stato indirizzato sulla seguente pagina.



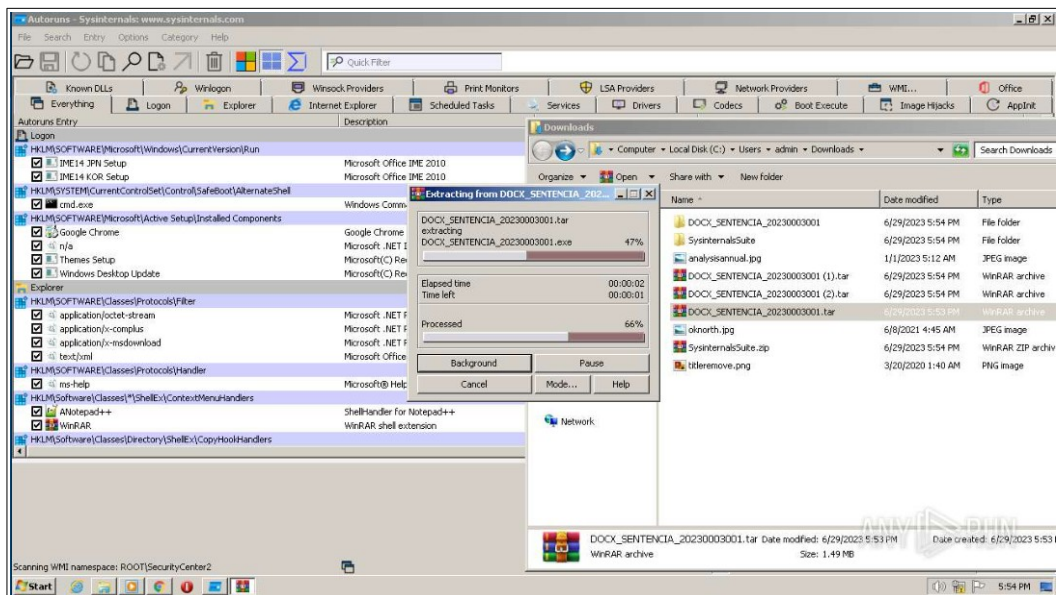
Senza chiudere la pagina originale, ha aperto una seconda scheda ed ha cercato online Sysinternals, uno strumento di diagnostica di Microsoft ed ha avviato il download.



Mentre veniva scaricato Sysinternals, è stato avviato automaticamente il download di un secondo file eseguibile.



Sia Sysinternals che il file potenzialmente malevolo sono stati decompressi ed eseguiti dall'utente. Dalla schermata sottostante possiamo notare che i file DOCX_SENTENCIA_20230003001.tar sono tre, questo implica che la pagina malevola sia ancora aperta e che stia continuando ad inviare il file potenzialmente malevolo al PC host.



L'attività è stata segnalata come malevola da Anyrun, senza un'analisi approfondita dal PC dell'utente non è possibile decretare con certezza cosa fosse contenuto nell'eseguibile. L'utente ha comunque commesso diverse azioni gravi dal punto di vista della sicurezza dell'azienda, il suo computer dovrà essere messo in quarantena ed analizzato accuratamente prima di poter essere restituito o di poter accedere nuovamente alla rete aziendale.

Pratica extra

Installare Wazuh come VM e configurare Kali come user-agent.

