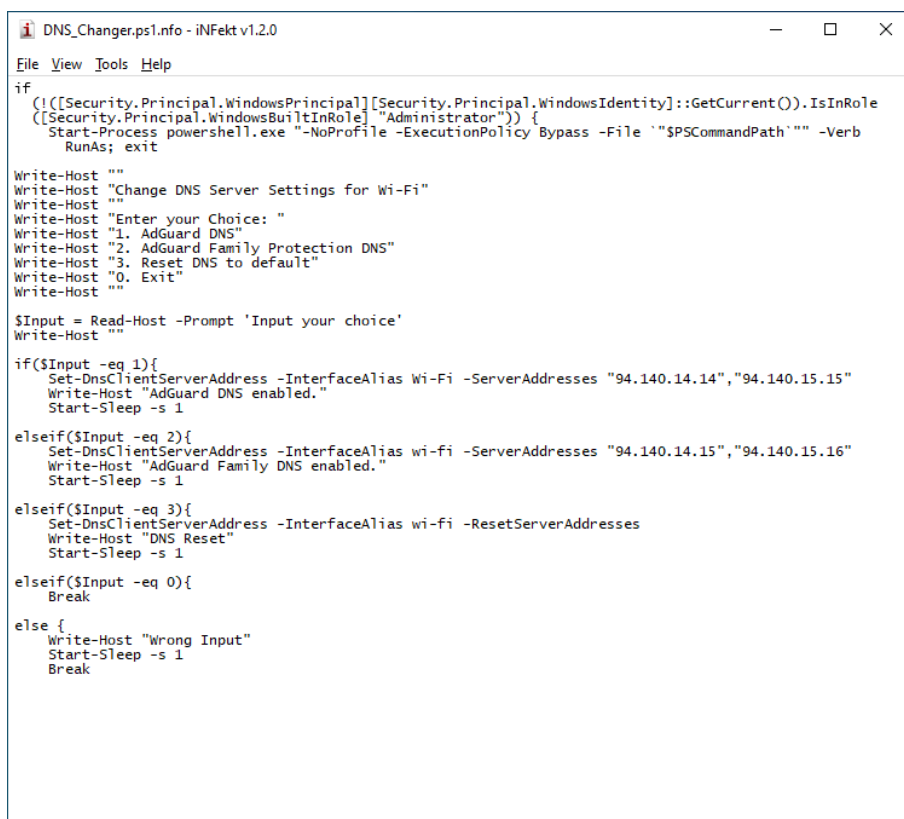


<https://tinyurl.com/linklosco1>

Nel report fornitoci da anyrun sono state rilevate diverse attività sospette. In particolare, è stato segnalato un bypass dell'esecuzione della policy del controllo utente di Windows, consentendo l'esecuzione di comandi potenzialmente dannosi. È stato infatti rilevato l'utilizzo di uno script PowerShell atto all'automazione processi ma che potrebbe nascondere un comportamento potenzialmente malevolo a livello del sistema. Inoltre, sempre il processo **powershell.exe**, ha bypassato le impostazioni del profilo predefinite, consentendo l'esecuzione di comandi elevati senza restrizioni. È stata anche rilevata la lettura delle impostazioni Internet, che a prima vista suggerirebbe un possibile interesse nel raccogliere informazioni sulla connettività e le configurazioni di rete. Un'altra attività sospetta la si può vedere sui processi **powershell.exe** e **firefox.exe** che vengono avviati senza interazione diretta dell'utente. Ciò potrebbe indicare un comportamento anomalo e potenzialmente dannoso. Tutto ciò sembra nascere dall'avvio dello script PowerShell citato in precedenza.

Questo potrebbe indicare l'utilizzo di un file dannoso o l'esecuzione di ulteriori attività sospette. Andiamo quindi a recuperare il file in questione e diamo un'occhiata al codice.



```
File View Tools Help
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
}
```

Il codice non è da considerarsi malevolo di per sé; anche gli indirizzi DNS sono effettivamente quelli forniti dal servizio AdGuard. In uno scenario aziendale, si potrebbe ipotizzare che lo script PowerShell sia stato scaricato e poi lanciato (con molta ingenuità) dall'utente nel tentativo di bypassare le policies di blocco sulla navigazione imposte dall'azienda. Per rimediare a ciò si andrà quindi a rimuovere il file in questione e verranno ripristinate le impostazioni di rete come da policy aziendale. Questo comportamento ci fa capire quanto sia importante l'educazione dei dipendenti per evitare di ritrovarsi in situazioni simili.

<https://tinyurl.com/linklosco2>

Durante la scansione su anyrun sono stati individuati diversi comportamenti sospetti e potenzialmente dannosi. Dall'analisi, sono stati rilevati processi compromessi tra cui **autoruns.exe** (PID: 4056) e **procexp.exe** (PID: 3476) che sono stati sovrascritti da altre applicazioni, indicando un possibile tentativo di camuffare una quasi certa attività malevola.

Inoltre, il processo **DOCX_SENTENCIA_20230003001.exe** (PID: 4040, 3912, 2432, 312) è stato avviato ed eseguito tramite il compilatore **csc.exe** (PID: 3824), sollevando preoccupazioni sulla presenza di possibile codice dannoso creato ed eseguito tramite quest'ultimo.

Anche il processo **winrar.exe** (PID: 1944) ha mostrato comportamenti sospetti, come la creazione di file con nomi simili a quelli dei file di sistema; mentre il processo **cmd.exe** (PID: 3604, 3200, 2628, 2960) ha eseguito comandi elevati tramite prompt, suggerendo un possibile tentativo di compromissione del sistema.

È stato anche individuato l'utilizzo del malware **remcos**, un noto **RAT (Remote Access Trojan)** utilizzato per il controllo remoto non autorizzato dei sistemi. Il malware sembra interagire con il compilatore **csc.exe** (PID: 3824) attraverso lo sfruttamento dei dump di memoria, confermando la presenza del trojan nel sistema.

Altri processi come **chrome.exe**, **wmpnscfg.exe** e **autoruns.exe** sono stati coinvolti nell'esecuzione sia automatica che manuale di file scaricati potenzialmente dannosi.

In sintesi, l'analisi ha rivelato la presenza di un attacco RAT nel sistema analizzato, con l'utilizzo di processi compromessi e comportamenti dannosi atti ad eludere le difese del sistema e interagire con applicazioni e servizi del sistema.

Per rimediare all'attacco, è necessario isolare il sistema compromesso, rimuovere il malware, applicare patch di sicurezza, analizzare i log, monitorare il sistema, educare gli utenti, implementare controlli di accesso e autenticazione ed effettuare backup regolari dei dati critici.