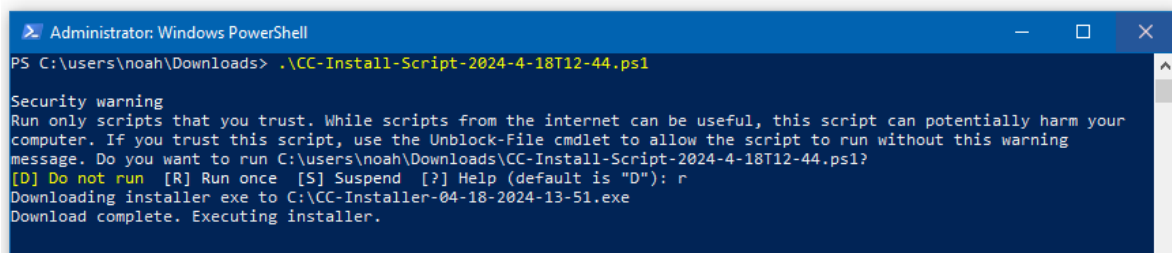


Visão Geral do Script de Instalação

1. O instalador mais recente é baixado de

`https://installerfiles.rpp.cybercrucible.com/installers/64/installer-cli.exe`

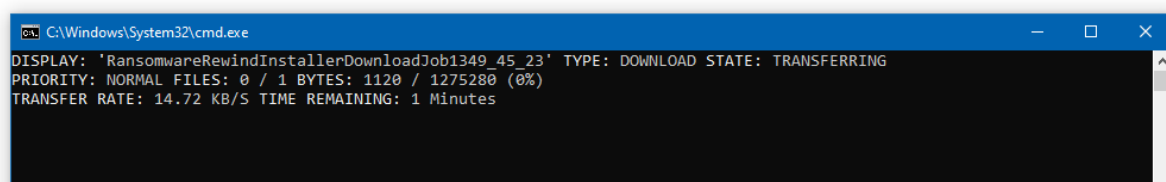
1. Os scripts de instalação PowerShell (PS1) usarão uma instância WebClient.



```
Administrator: Windows PowerShell
PS C:\users\noah\Downloads> .\CC-Install-Script-2024-4-18T12-44.ps1

Security warning
Run only scripts that you trust. While scripts from the internet can be useful, this script can potentially harm your
computer. If you trust this script, use the Unblock-File cmdlet to allow the script to run without this warning
message. Do you want to run C:\users\noah\Downloads\CC-Install-Script-2024-4-18T12-44.ps1?
[D] Do not run [R] Run once [S] Suspend [?] Help (default is "D"): r
Downloading installer exe to C:\CC-Installer-04-18-2024-13-51.exe
Download complete. Executing installer.
```

2. Os scripts de instalação Batch (BAT) usarão o BitsAdmin, ou JScript caso o BitsAdmin falhe.



```
C:\Windows\System32\cmd.exe
DISPLAY: 'RansomwareRewindInstallerDownloadJob1349_45_23' TYPE: DOWNLOAD STATE: TRANSFERRING
PRIORITY: NORMAL FILES: 0 / 1 BYTES: 1120 / 1275280 (0%)
TRANSFER RATE: 14.72 KB/S TIME REMAINING: 1 Minutes
```

2. O instalador é executado e recebe o ID do grupo e a autenticação de cliente fornecidos no seu script.

1. Opcionalmente, adicione `--reuse-agent-by-machine-name` à execução do exe, para que o instalador reutilize o objeto de agente e a licença de um agente instalado anteriormente com o mesmo nome NetBIOS.

3. O instalador verifica as condições de instalação necessárias

1. Está sendo executado com privilégios de Administrador.
2. A máquina está executando uma [versão compatível do Windows](#).
3. Não há outro instalador já em execução.
4. O agente ainda não está instalado.

4. O instalador verifica se a máquina consegue se comunicar com os [servidores necessários](#).

1. Amazon oAuth 2.0 em `ransomwarerewind-agents.auth.us-west-2.amazoncognito.com`
2. Backend da Cyber Crucible em `agent.tasking.rpp.cybercrucible.com`

5. Os arquivos do agente são baixados de `installerfiles.rpp.cybercrucible.com` via HTTPS.
6. O agente é instalado e iniciado.