Como Instalar o Cyber Crucible

Firewalls que bloqueiam o acesso da autoridade certificadora CRL/OCSP (Modo DMZ)

Como Instalar o Cyber Crucible

A instalação do Cyber Crucible é simples. Faça login na aplicação web em https://dashboard.cybercrucible.com

Vá até a página Agents e clique no botão Download Agent.

85131265.png?width=680
Após clicar no botão, o seguinte modal aparece:

85229569.png?width=340
Selecione o grupo no qual você deseja que o(s) agente(s) que está(ão) sendo instalado(s) apareça(m) inicialmente.

Se o grupo não aparecer na lista, você precisará criar o grupo ou pedir ao administrador do grupo que o adicione ao grupo existente.

Após a instalação, você sempre pode alterar o grupo no qual um agente está, ou de vários agentes de uma vez. Normalmente, é mais fácil configurar a associação ao grupo antes da implantação em massa do que organizar os agentes após a instalação.

Permissões Necessárias

É necessário acesso administrativo a uma máquina para instalar e carregar o serviço e o driver do Cyber Crucible.

A instalação por script baixa e configura especificamente o instalador para o local padrão C:\. O script deve ser executado como um usuário ou função que tenha permissão para o local de download e execução.

Assim, é necessário um usuário com permissão para usar C:\ durante a instalação, ou o script (detalhado abaixo) precisa ser ajustado para baixar e executar em um local diferente.

Instalação via GUI

Este método de instalação permite que o usuário configure e instale manualmente uma instalação.

Este método de instalação exige que um usuário com permissões para instalar no grupo especificado consiga fazer login.

É melhor utilizado para 1 ou 2 instalações, por um único usuário.

Instalação via Script

Este é, de longe, o método de instalação mais comum.

Com este método, a aplicação web do Cyber Crucible configura automaticamente o processo de instalação e o bootstrapping seguro do agente na aplicação web.

Um arquivo batch do Windows é utilizado. Embora existam outros métodos de instalação mais complexos possíveis, este método possui a maior compatibilidade com ferramentas de Gerenciamento Remoto.

O arquivo batch pode ser executado como um usuário com as permissões apropriadas (geralmente administrador), ou copiado/colado em sua ferramenta de implantação automática preferida.

Abaixo está uma análise técnica do conteúdo do arquivo batch, que pode ser configurado de acordo com suas necessidades.

Análise Detalhada do Script de Instalação

O identificador do grupo selecionado durante a criação do script é inserido no script, assim como o token oauth necessário para que os agentes ingressem no grupo específico.

47480849.png?width=680
Observe que este token de autenticação oAuth não está associado à aplicação web, nem a nenhum usuário. Ele não pode ser usado para fazer chamadas REST à API da aplicação web.

Em alguns ambientes, as permissões podem ser obtidas automaticamente. Isso geralmente ocorre em circunstâncias em que um usuário está executando o script de instalação clicando nele, em vez de acesso programático. Em ambientes empresariais ou ferramentas de implantação automatizada, é provável que isso não seja executado.

47480857.png?width=680
Neste próximo local no script, o local do arquivo a partir do qual o instalador pode ser baixado e executado pode ser personalizado.

É altamente recomendável tornar este local local à máquina na qual a ferramenta está sendo instalada. Várias máquinas baixando instaladores para o mesmo local causarão falhas e

sobrescritas.

Observe que a reinicialização automática por meio do script de instalação não é utilizada por padrão. Isso ocorre porque a reinicialização automatizada neste script não possui o gerenciamento necessário para agendar instalações para um horário específico, métodos de desligamento limpo que verificam se o usuário está atualmente conectado ou executando aplicativos, ou para avisar o usuário sobre uma reinicialização iminente.

47513621.png?width=680
Esta próxima seção realiza o download e a nomeação personalizada do instalador na máquina. Observe que a data e a hora são usadas para fornecer exclusividade ao arquivo de instalação, caso ele seja baixado múltiplas vezes com configurações ou versões diferentes.

Bitsadmin é um utilitário do Windows que tenta baixar arquivos sem impactar negativamente a máquina caso o Sistema Operacional esteja atualmente sob carga pesada.

47448109.png?width=680
Em alguns ambientes, o protocolo Bits está desativado. Além disso, o bits pode estar em um estado não operacional devido a um erro do Windows. Caso o download via Bits falhe, a próxima seção usa um método alternativo (.net JSC) para baixar o arquivo do instalador. Este código só é executado se o downloader bits anterior falhar.

47415316.png?width=680
Após o download do instalador, esta seção final do script executa o instalador. Observe que a personalização dos argumentos de linha de comando deve ser testada, para garantir que as configurações e proteções do installer.exe estejam alinhadas com os argumentos de linha de comando fornecidos aqui.

Por favor, abra um chamado de suporte caso configurações adicionais sejam necessárias, ou para ambientes avançados, como configurações de SSL man in the middle.

47480877.png?width=680
Observe que a reinicialização não é necessária e está comentada, não sendo executada. Raramente, mais comumente em versões mais antigas do Windows, os drivers não se registravam nem carregavam no sistema operacional, apesar de instruídos a fazê-lo pelo instalador. Nesses cenários, o método mais fácil de garantir que o driver seja carregado é exportar os agentes para um documento Excel e procurar nomes de máquinas ausentes na sua lista de ativos. Se todas as instalações estiverem em um novo grupo, a contagem de agentes também pode ser usada.

47480889.png?width=680
Esta seção, no final do script de instalação, é a função usada para baixar o instalador usando JSC, caso necessário. Ela só é executada se o .net JSC for utilizado para baixar o instalador, como no caso de falha do bits.

47480895.png?width=680

Como localizo os logs de instalação?

Os instaladores CLI headless emitem seu status e logs tanto para `stdout` quanto para um arquivo de log, localizado no diretório local do executável do instalador. Por padrão, ao usar um script pré-empacotado, como os scripts ps1 ou bat baixados de https://dashboard.cybercrucible.com, o arquivo de log estará localizado na raiz da unidade C:.

Os arquivos de log de instalação são nomeados `cc_installer.log`

Os instaladores GUI não produzem os mesmos arquivos de log, pois não são headless, e todos os logs são exibidos na seção de texto rolável da janela do GUI.

Forçar a Implantação do Instalador no Domínio AD

Em alguns ambientes frágeis, particularmente se estiver se recuperando de um ataque recente ou de uma interrupção, as implantações normais de RMM e/ou SCCM podem não ser uma opção. Aqui você encontrará um script que pode servir como modelo de como seria possível forçar a implantação de uma instalação da CC em um ambiente de active directory.

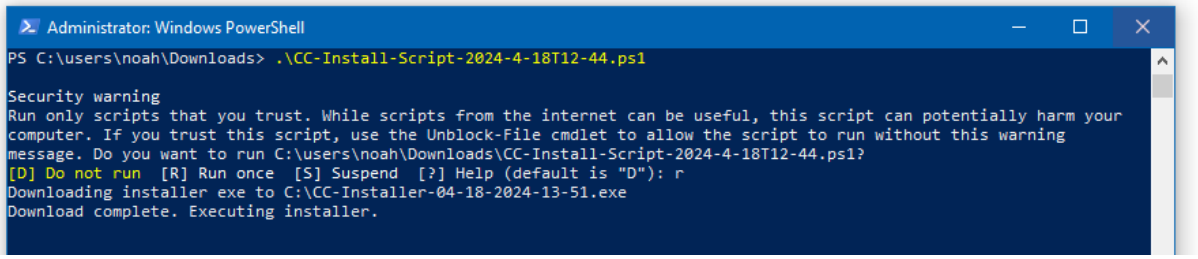
Observação: Este script provavelmente precisará ser adaptado para o seu caso de uso, e requer credenciais de domínio para ser executado. Espera-se que este script seja executado diretamente em um controlador de domínio (primário).

Etapas para execução

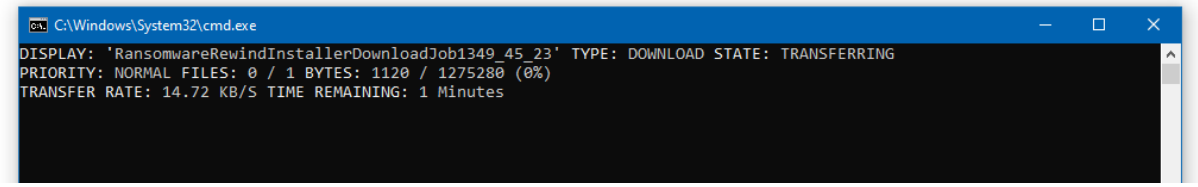
1. Atualize a variável `$install_targets` com uma lista de nomes de máquinas (NETBIOS ou nomes de host semelhantes)
2. Baixe um script instalador ps1 ‘normal’ a partir do painel do Cyber Crucible
3. Atualize as variáveis no script push_installer_ad.ps1 para que sejam iguais às variáveis específicas do seu grupo obtidas no script do painel
    1. `${GroupId}`
    2. `${ClientAuth}`
    3. quaisquer variáveis `--rest-pub-key`
4. Baixe um executável nativo de CLI a partir do painel do Cyber Crucible
    1. Coloque o CLI em um compartilhamento de rede, ou em algum local acessível a todas as máquinas que serão instaladas
        1. Isso evita que cada máquina precise gastar tempo e largura de banda para baixar novamente o mesmo exe
        2. O mesmo exe pode ser executado para diferentes sistemas operacionais, pois o instalador irá buscar os arquivos de serviço/driver/instalação relevantes para o SO detectado e a função da máquina.
    2. Defina `${OutputFilePath` como o caminho do CLI em um compartilhamento de rede
5. Possivelmente remova a verificação online por ICMP (se não for necessária / inválida para o seu ambiente)
6. Execute o script com `-credential`
    1. por exemplo, `./push_installer_ad.ps1 -credential ad1\kyle`

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.



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



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.

Instalar com SCCM

Instalar o Cyber Crucible com o SCCM não é diferente de qualquer outro pacote de software. Os pontos-chave para a implantação via SCCM são:

1. Implante com o script PS1 pré-criado, baixado de https://dashboard.cybercrucible.com
2. Procure pelo serviço **Cyber Crucible Agent** em execução, ou existente no disco, como método de detecção. O local padrão do serviço do agente é **C:\Program Files\CyberCrucible\service.exe**
    1. Opcionalmente, você também pode verificar a existência da chave de registro **HKLM\Software\CyberCrucibleAgent**, mas observe que, após uma desinstalação, essa chave pode ainda estar presente.

Etapas de Configuração Padrão

1. Crie uma Aplicação, e **não** um pacote
2. Especifique manualmente a configuração

image-20250807-175116.png

3. Configure o nome da aplicação, nome do fornecedor, descrição, etc.
4. Configure o Tipo de Implantação e especifique **Instalador por Script**

image-20250807-175303.pngimage-20250807-175332.png

5. Especifique o local do script, provavelmente um compartilhamento de rede, por exemplo, **\\cc-dc01\share**
6. Especifique o programa de instalação para executar o ps1 fornecido, por exemplo, `Powershell.exe -file “CC-Install-Script-2025-8-7T13-55.ps1`
    1. Observe o carimbo de data no nome do script e altere-o para o seu
    2. Não é recomendado sobrescrever as políticas do PowerShell, mas, dependendo da sua configuração, pode ser necessário especificar `-executionpolicy Bypass` ou similar
7. Adicione um Método de Detecção clicando em “Add Clause”
    1. Consulte os métodos de detecção recomendados no topo desta página
8. Especifique as configurações de implantação de UX
    1. Como a implantação do Cyber Crucible não requer reinicialização, os requisitos de instalação e logon ficam a critério da sua organização

image-20250807-175906.png

9. Selecione Avançar / Concluir até conseguir fechar o assistente.