Cenário de Treinamento - Roubo de Identidade

Nome do Grupo

Dados de Treinamento - Roubo de Identidade (Redline)

Cenário

Neste cenário de treinamento, executaremos um malware do tipo “stealer” para realizar a primeira etapa de um ataque, o roubo de credenciais. Diferente do cenário de **RAT**, este não utiliza os mesmos comportamentos que o ransomware. Em vez disso, faz parte das crescentes capacidades de proteção de identidade da Cyber Crucible.

Frequentemente, antes mesmo de ocorrer uma extorsão, os primeiros passos que um atacante realiza são se propagar pela rede e obter acesso ao maior número possível de credenciais. Em alguns casos, trata-se de uma combinação de nome de usuário/senha do AD; em outros, são chaves de API capturadas de sessões de navegador.

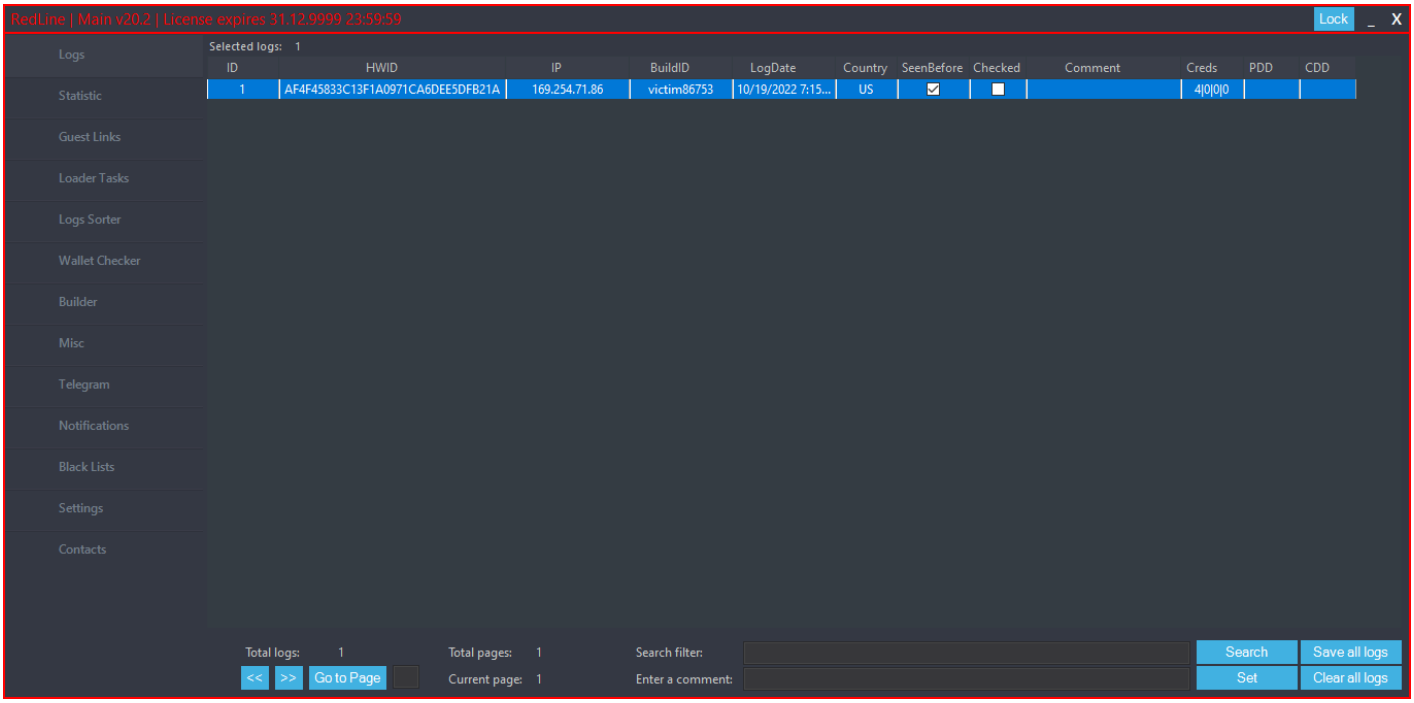
Identificando

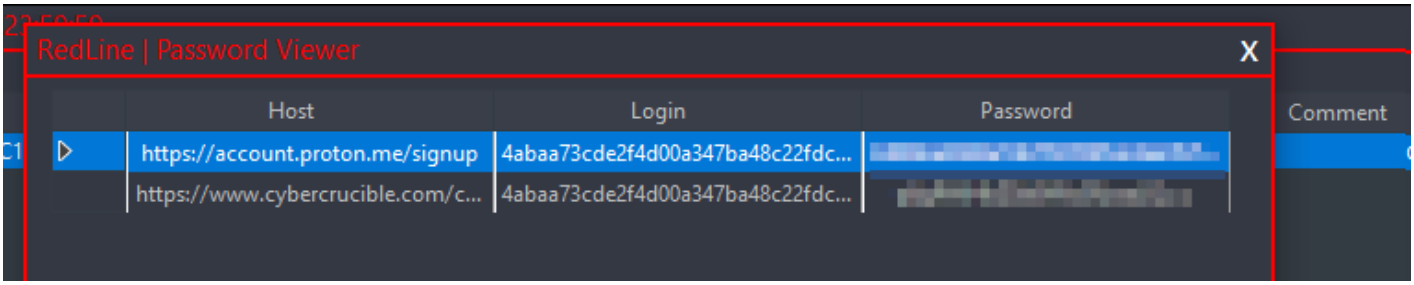
Por ora, vamos analisar como o acesso anormal se apresenta ao administrador.

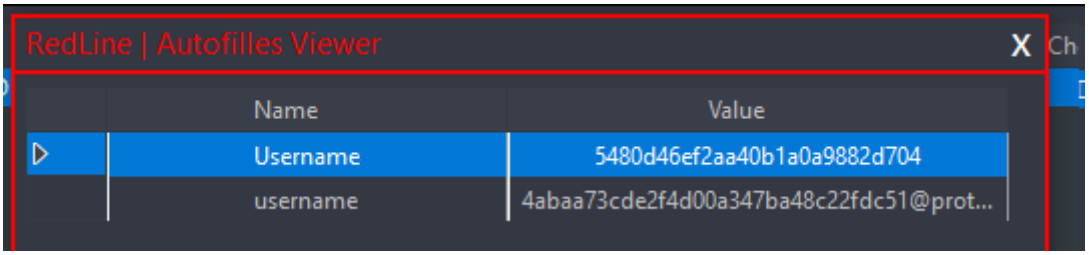
Accessing Program Path	Untrusted Remote Threads	Modified Memory	No Trusted Cert
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True

Os acessos a dados de identidade são muito claros e objetivos: se os administradores não reconhecem um programa, ele não deveria estar acessando esses dados! Isso já se destaca imediatamente como algo suspeito.

Qual é o outro lado disso que o atacante vê? Texto puro!







Essas respostas não são como as respostas de eventos tradicionais de extorsão de dados, portanto não são ações de suspensão automática. Em vez disso, são mais semelhantes a injeções de processo, nas quais a Cyber Crucible não interferiu. À medida que nossas análises têm evoluído, aprendemos como é o acesso “normal” a repositórios de identidade para diversos tipos de aplicações. Até 2023, habilitaremos nosso recurso de proteção, que restringirá o acesso, em nível de kernel, a diversas formas de bancos de dados de identidade, permitindo o acesso apenas ao software associado.

Documentação relevante

- **Injeção de Processo**
- Mitre T1559 - A comunicação entre processos (Inter-Process communication) pode fornecer controle sobre o processo de destino a partir do injetor, uma vez concluída a injeção.
- Mitre T1106 - As APIs nativas costumam ser o acesso mais próximo à funcionalidade do sistema operacional para acessar arquivos, executar processos e muito mais.
- Mitre T1569 - Injetar em um serviço de sistema, como um `svchost` existente, pode disfarçar o código malicioso para que seja reportado como sendo executado a partir de um processo bem conhecido e confiável.
- Mitre T1055 - Injeção de processo, geralmente usada para executar código malicioso em um processo de destino, permitindo que o processo original continue em execução.
- Mitre T1543 - Criar ou modificar um processo do sistema pode disfarçar o código malicioso como um processo de sistema normal e confiável, evitando a detecção por malware.
- Mitre T1555 - Credenciais armazenadas em gerenciadores ou navegadores não criptografados podem ser usadas para obter acesso a dados privilegiados.
- Mitre T1212 - As credenciais podem ser roubadas ao explorar softwares vulneráveis que não criptografam as credenciais inseridas por um usuário.

Revision #1
Created 2026-07-24 05:13:33 UTC by Dennis Underwood
Updated 2026-07-24 05:13:33 UTC by Dennis Underwood