# Training Scenario - Identity Theft

## Group Name

**Training Data - Identity Theft (Redline)**

## Scenario

In this training scenario, we will execute a piece of “stealer” malware in order to perform the first stage of an attack, credential theft. Unlike the **RAT** scenario, this one does not use the same behaviors as ransomware. Instead, this is a part of Cyber Crucible’s growing identity protection capabilities.

Often before an extortion even occurs, the first steps an attacker will do are to worm around the network and gain access to as many credentials as possible. In some cases this is an AD username/password combo, in other cases they are API keys grabbed out of browser sessions.

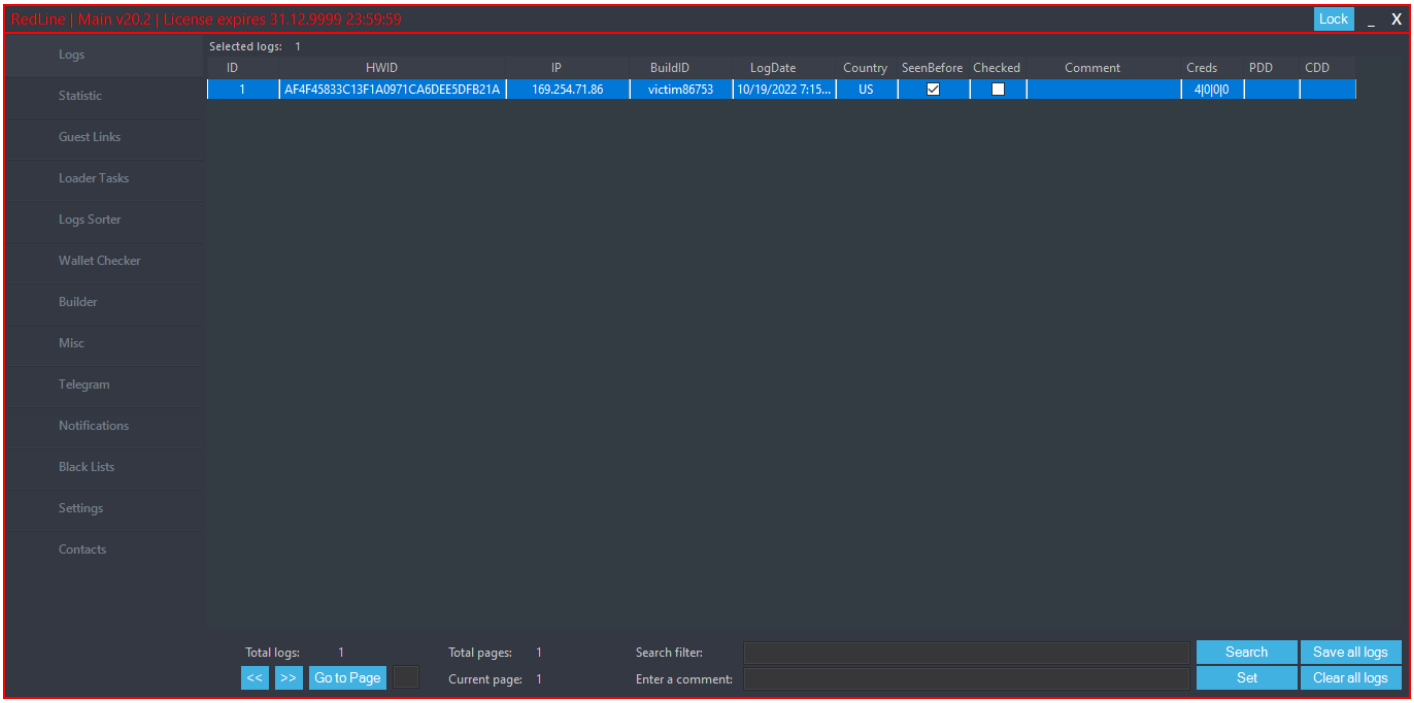
## Identifying it

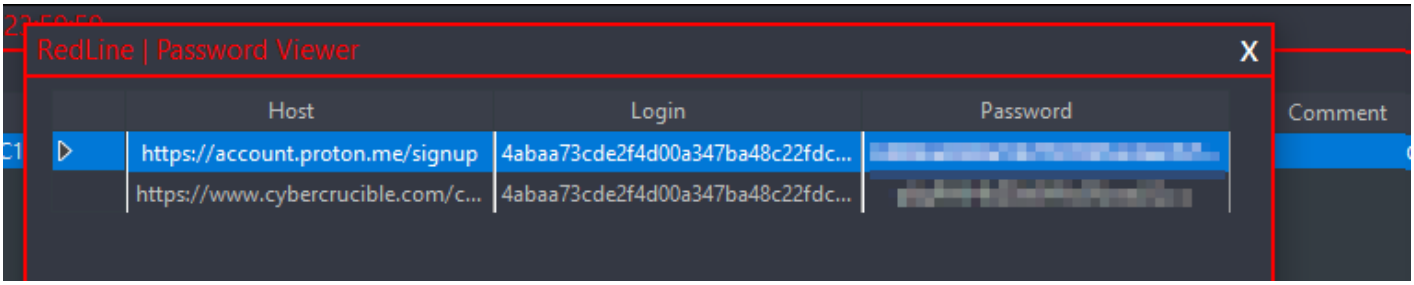
For now, lets dig in to some of what abnormal access looks like to the admin.

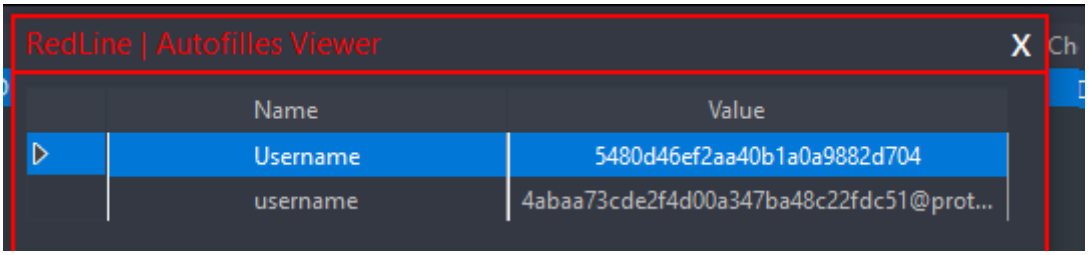
| Accessing Program Path | Untrusted Remote Threads | Modified Memory | No Trusted Cert |
|---|---|---|---|
| C:\Users\User\Desktop\redline.exe | False | False | True |
| C:\Users\User\Desktop\redline.exe | False | False | True |
| C:\Users\User\Desktop\redline.exe | False | False | True |
| C:\Users\User\Desktop\redline.exe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

Identity data accesses are very cut and dry, if the admins don't recognize a program, it shouldn't be accessing that data! This immediately stands out as something suspicious going on.

What's the flip side of this the attacker sees? Plaintext!






These responses are not responses like traditional data extortion events, so they are not actions of automated suspension. Instead, they are more like process injections, where Cyber Crucible did not stand in the way. As our analytics have been growing out, we have learned what “normal” access to identity stores look like for various types of applications. By 2023 we will enable our protection feature, which will restrict access, at the kernel level, to various forms of identity databases and only allow the associated software to access them.

# Relevant documentation

- **Process Injection**
- Mitre T1559 - Inter-Process communication can provide control over the target process from the injector once the injection is complete.
- Mitre T1106 - Native APIs are often the closest access to operating system functionality for accessing files, running processes, and more.
- Mitre T1569 - Injecting into a system service such as an existing `svchost` can disguise malicious code to be reported as running from a well known and trusted process.
- Mitre T1055 - Process injection, usually used to run malicious code in a target process while allowing the original process to continue.
- Mitre T1543 - Creating or modifying a system process can disguise malicious code as a normal, trusted system process from malware detection.
- Mitre T1555 - Stored credentials from unencrypted managers or browsers may be used to gain access to privileged data.
- Mitre T1212 - Credentials could be stolen by taking advantage of vulnerable software that does not encrypt credentials inputted by a user.

---

Revision #2
Created 2026-07-13 18:49:15 UTC by Dennis Underwood
Updated 2026-07-13 18:49:19 UTC by Dennis Underwood