Trainingsszenario – Identitätsdiebstahl

Gruppenname

Trainingsdaten - Identitätsdiebstahl (Redline)

Szenario

In diesem Trainingsszenario führen wir ein Stück „Stealer“-Malware aus, um die erste Phase eines Angriffs, den Diebstahl von Zugangsdaten, durchzuführen. Im Gegensatz zum **RAT**-Szenario verwendet dieses nicht dieselben Verhaltensweisen wie Ransomware. Stattdessen ist dies Teil der wachsenden Identitätsschutzfähigkeiten von Cyber Crucible.

Oft, noch bevor es überhaupt zu einer Erpressung kommt, bestehen die ersten Schritte eines Angreifers darin, sich wurmartig durch das Netzwerk zu bewegen und Zugriff auf möglichst viele Zugangsdaten zu erlangen. In manchen Fällen handelt es sich dabei um eine AD-Benutzername/Passwort-Kombination, in anderen Fällen um API-Schlüssel, die aus Browsersitzungen entwendet werden.

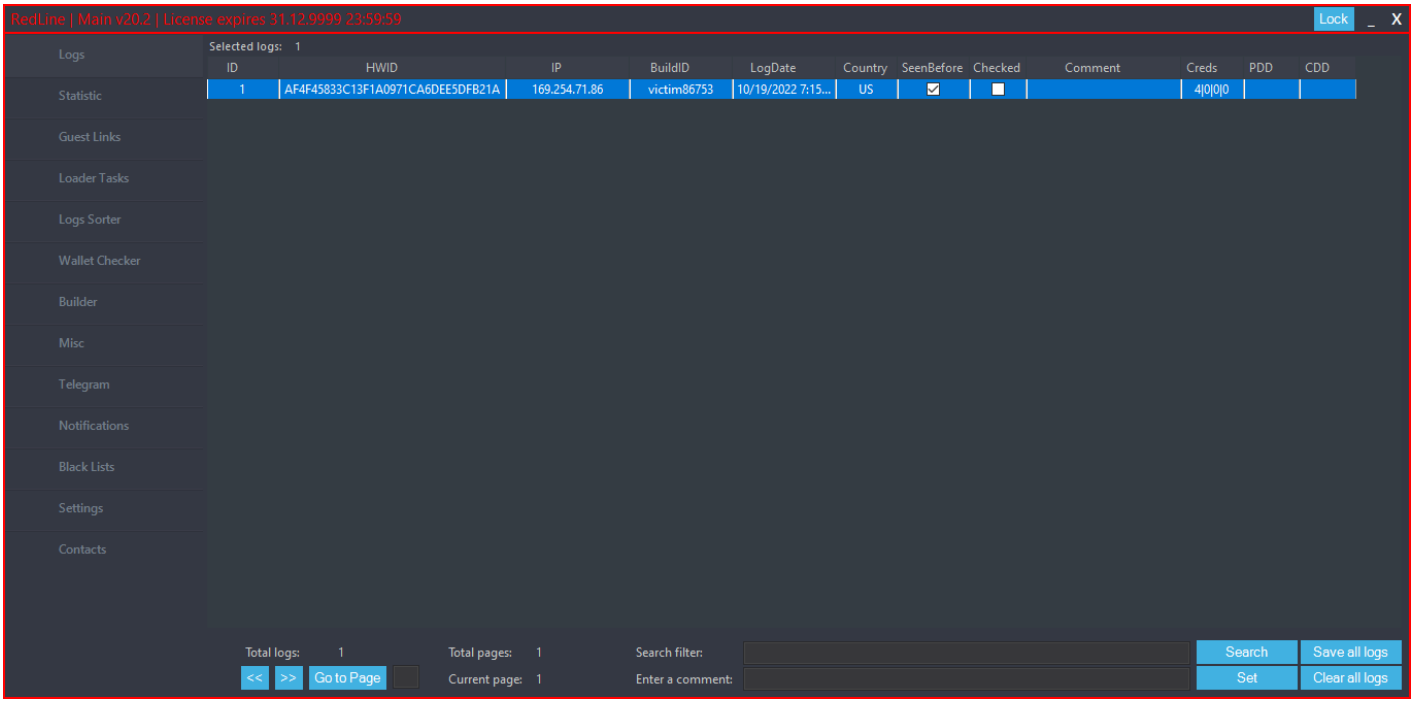
Erkennung

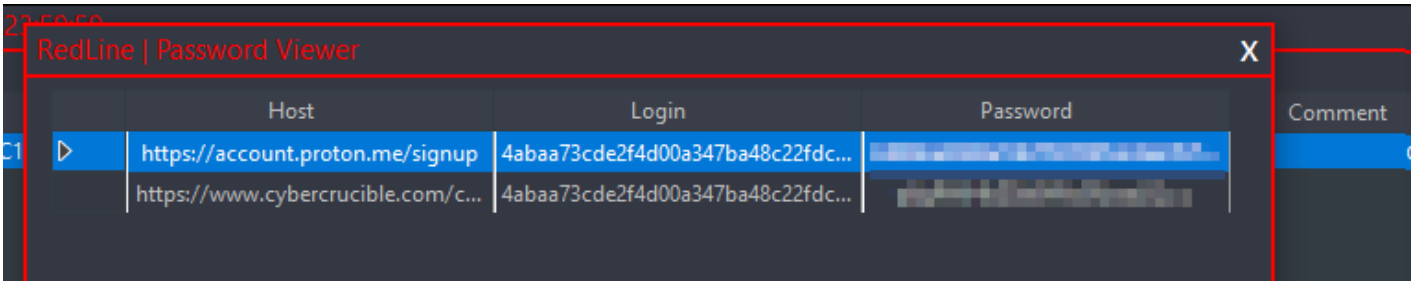
Schauen wir uns nun genauer an, wie abnormaler Zugriff für den Administrator aussieht.

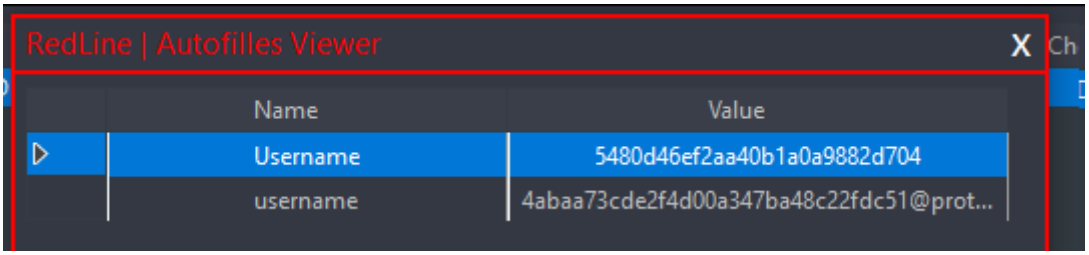
Accessing Program Path	Untrusted Remote Threads	Modified Memory	No Trusted Cert
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe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

Zugriffe auf Identitätsdaten sind sehr eindeutig: Wenn die Administratoren ein Programm nicht kennen, sollte es keinen Zugriff auf diese Daten haben! Dies fällt sofort als etwas Verdächtiges auf.

Wie sieht die Kehrseite davon aus der Sicht des Angreifers aus? Klartext!







Diese Reaktionen sind keine Reaktionen wie bei traditionellen Datenerpressungsereignissen, daher handelt es sich nicht um Maßnahmen einer automatisierten Suspendierung. Stattdessen ähneln sie eher Prozessinjektionen, bei denen Cyber Crucible nicht im Weg stand. Da unsere Analysen stetig weiterentwickelt wurden, haben wir gelernt, wie „normaler“ Zugriff auf Identitätsspeicher für verschiedene Arten von Anwendungen aussieht. Bis 2023 werden wir unsere Schutzfunktion aktivieren, die den Zugriff auf verschiedene Formen von Identitätsdatenbanken auf Kernel-Ebene einschränkt und nur der zugehörigen Software den Zugriff darauf erlaubt.

Relevante Dokumentation

- **Process Injection**
- Mitre T1559 - Interprozesskommunikation kann dem Injektor die Kontrolle über den Zielprozess ermöglichen, sobald die Injektion abgeschlossen ist.
- Mitre T1106 - Native APIs bieten oft den direktesten Zugriff auf Betriebssystemfunktionen, um auf Dateien zuzugreifen, Prozesse auszuführen und mehr.
- Mitre T1569 - Die Injektion in einen Systemdienst wie einen bestehenden `svchost` kann bösartigen Code so tarnen, dass er als von einem bekannten und vertrauenswürdigen Prozess ausgeführt erscheint.
- Mitre T1055 - Prozessinjektion, meist verwendet, um bösartigen Code in einem Zielprozess auszuführen, während der ursprüngliche Prozess weiterläuft.
- Mitre T1543 - Das Erstellen oder Verändern eines Systemprozesses kann bösartigen Code als normalen, vertrauenswürdigen Systemprozess vor der Malware-Erkennung tarnen.
- Mitre T1555 - Gespeicherte Zugangsdaten aus unverschlüsselten Passwort-Managern oder Browsern können genutzt werden, um Zugriff auf privilegierte Daten zu erlangen.
- Mitre T1212 - Zugangsdaten könnten gestohlen werden, indem eine verwundbare Software ausgenutzt wird, die vom Benutzer eingegebene Zugangsdaten nicht verschlüsselt.

Revision #1
Created 2026-07-24 03:56:52 UTC by Dennis Underwood

Updated 2026-07-24 03:56:52 UTC by Dennis Underwood