Scénario de formation - Vol d'identité

Nom du groupe

Données de formation - Vol d'identité (Redline)

Scénario

Dans ce scénario de formation, nous allons exécuter un logiciel malveillant de type « voleur » (stealer) afin d'exécuter la première étape d'une attaque, le vol d'identifiants. Contrairement au scénario **RAT**, celui-ci n'utilise pas les mêmes comportements qu'un rançongiciel. Il s'agit plutôt d'une partie des capacités croissantes de Cyber Crucible en matière de protection de l'identité.

Souvent, avant même qu'une extorsion ne se produise, les premières étapes qu'un attaquant effectue consistent à se propager dans le réseau et à obtenir l'accès à autant d'identifiants que possible. Dans certains cas, il s'agit d'une combinaison nom d'utilisateur/mot de passe AD, dans d'autres cas, il s'agit de clés API récupérées à partir de sessions de navigateur.

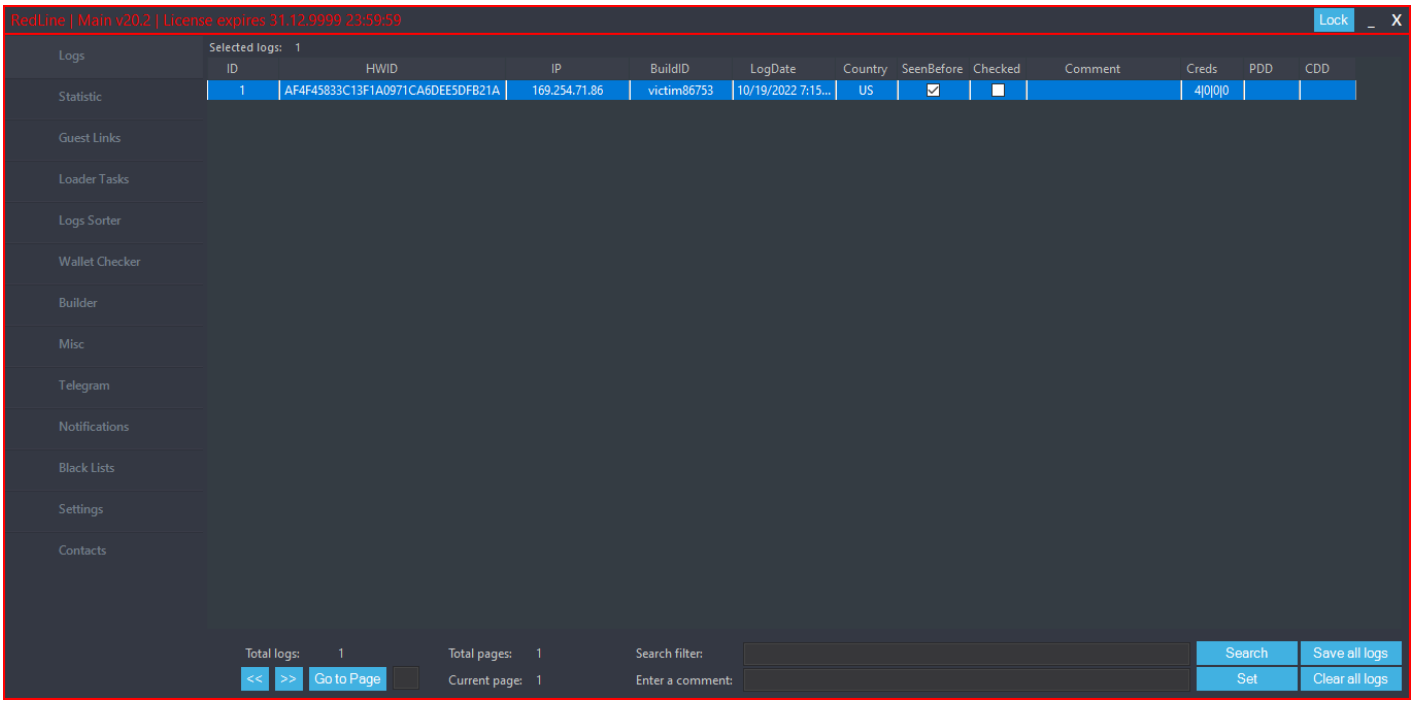
Identification

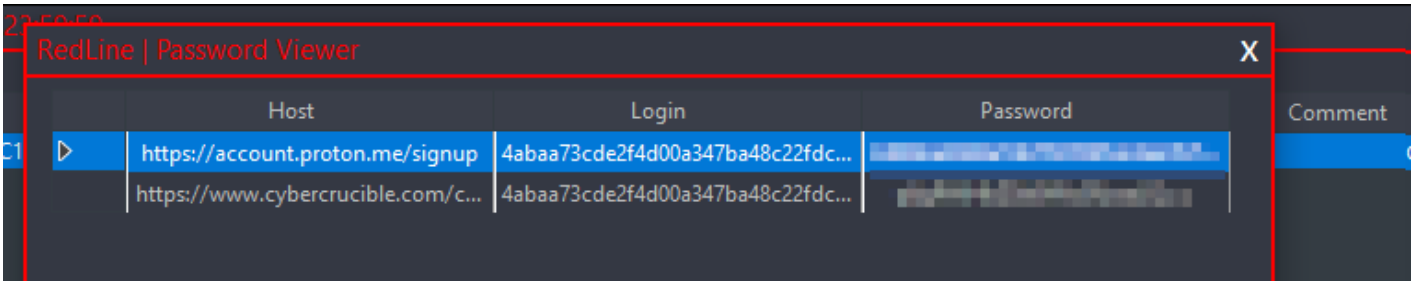
Pour l'instant, examinons de plus près à quoi ressemble un accès anormal pour l'administrateur.

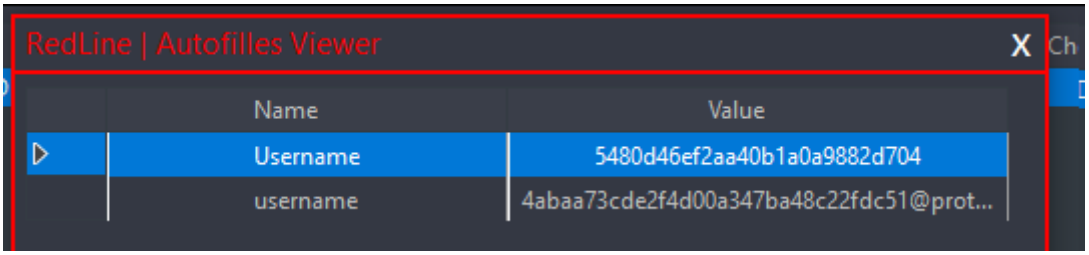
Accessing Program Path	Untrusted Remote Threads	Modified Memory	No Trusted Cert
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe	False	False	True
C:\Users\User\Desktop\redline.exe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

Les accès aux données d'identité sont très clairs et nets : si les administrateurs ne reconnaissent pas un programme, celui-ci ne devrait pas accéder à ces données ! Cela révèle immédiatement quelque chose de suspect en train de se produire.

Quel est l'autre côté de la médaille que voit l'attaquant ? Du texte en clair !







Ces réponses ne sont pas des réponses comme lors des événements traditionnels d'extorsion de données, elles ne sont donc pas des actions de suspension automatisée. Il s'agit plutôt d'injections de processus, où Cyber Crucible n'est pas intervenu. À mesure que nos analyses se sont développées, nous avons appris à quoi ressemble un accès « normal » aux magasins d'identité pour divers types d'applications. D'ici 2023, nous activerons notre fonctionnalité de protection, qui restreindra l'accès, au niveau du noyau, à diverses formes de bases de données d'identité et n'autorisera que le logiciel associé à y accéder.

Documentation pertinente

- **Injection de processus**
- Mitre T1559 - La communication inter-processus peut fournir un contrôle sur le processus cible depuis l'injecteur une fois l'injection terminée.
- Mitre T1106 - Les API natives constituent souvent l'accès le plus direct aux fonctionnalités du système d'exploitation pour accéder aux fichiers, aux processus en cours d'exécution, et plus encore.
- Mitre T1569 - L'injection dans un service système tel qu'un `svchost` existant peut déguiser un code malveillant afin qu'il soit signalé comme s'exécutant depuis un processus bien connu et de confiance.
- Mitre T1055 - Injection de processus, généralement utilisée pour exécuter du code malveillant dans un processus cible tout en permettant au processus d'origine de continuer.
- Mitre T1543 - Créer ou modifier un processus système peut déguiser un code malveillant en un processus système normal et de confiance afin d'échapper à la détection des logiciels malveillants.
- Mitre T1555 - Les identifiants stockés dans des gestionnaires ou des navigateurs non chiffrés peuvent être utilisés pour obtenir l'accès à des données privilégiées.
- Mitre T1212 - Les identifiants pourraient être volés en exploitant un logiciel vulnérable qui ne chiffre pas les identifiants saisis par un utilisateur.

Revision #1
Created 2026-07-24 06:21:57 UTC by Dennis Underwood
Updated 2026-07-24 06:21:57 UTC by Dennis Underwood