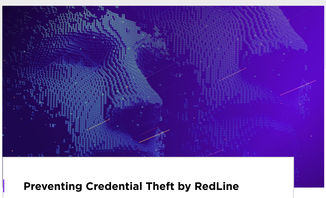

Preventing Credential Theft by RedLine Stealer Malware

November 10, 2021
By Gonjong Joshi and Chandan S

A credential-based attack occurs when an attacker steals credentials, extends privileges, and compromises critical data. Credential theft is the first stage of a lateral movement attack and stopping the attack early in the process can make a material impact on the success and damages incurred by an attacker.

RedLine Stealer malware was found to be used by attackers extensively to harvest saved credentials from applications such as browsers and windows credential manager. Several fake installers of renowned software have been reported for dropping the Redline Stealer malware. Using this tool, it is remarkably easy to retrieve and save credentials from any application. This malware when dropped, scans the affected endpoint for Crypto Wallets, Browser Login Credentials, Cookies, VPN client credentials and Instant Messaging Applications. A credential theft allows attackers access to a slew of other resources on the network. And much of these can be accessed by attackers without getting detected.

The Attivo ThreatStrike Credentials Protection hides and denies unauthorized access to applications credential store. For example, only Chrome will have access to its credential store, and all other applications won't. The product protects more than 80 of the most popular Windows applications that attackers target, with a plan to add more applications.

With RedLine Stealer gaining attention lately, Attivo research team tested the tool to see the level of Trust Issues attackers would face using such tools.

In the following section we first show how an attacker can easily grab such data using RedLine Stealer and then compare that with what happens when the same tool is run on a machine which is protected with Attivo Credentials Protection.

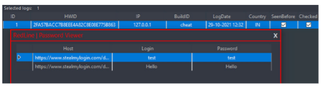

Figure 1: Credentials Stolen without Attivo's ThreatStrike Credential Protection

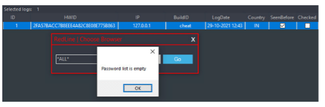

Figure 2: Credential Theft Prevented With Attivo's ThreatStrike Credential Protection

ThreatStrike Credential Protection from Attivo not only prevents malware from accessing production credentials, but also alerts users if such behavior is seen. The illustration below captures how alerts show up in the Events dashboard.

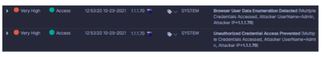

Figure 3: Event Level view of the Incident Occurred

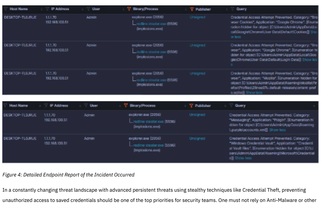

Figure 4: Detailed Endpoint Report of the Incident Occurred

In a constantly changing threat landscape with advanced persistent threats using stealthy techniques like Credential Theft, preventing unauthorized access to saved credentials should be one of the top priorities for security teams. One must not rely on Anti-Malware or other Endpoint Protection Platforms to prevent usage of tools like RedLine Stealer. There is always a new method available to evade the Endpoint Protection technologies.

Attivo Credentials Protection prevents credentials theft by denying access to unauthorized applications. To learn more about the Attivo Networks EDN Suite's new credential protection capability, read the press release here. For more information on the EDN Suite solution, go here.

Like this article? Follow us on LinkedIn, Twitter, YouTube or Facebook to see the content we post.

Read more about Cyber Security

- Detecting Brute Force Password Attacks
- Detecting Unconstrained Delegation Exposures in AD Environment
- Top 10 Ways to Protect Your Active Directory
- Protecting Your Active Directory from AdminSDHolder Attacks
- Detecting a Rogue Domain Controller – DCShadow Attack
- Rise in Identity-Based Attacks Drives Demand for a New Security Approach