Windows 1.4.3.3 Release

PLATFORM FEATURE UPDATE

Adlumin announced the winter release of its Windows 1.4.3.3 client with enhanced collection and stability. 1.4.3.3 is now available for download and testing.

The full release is scheduled for the week of December 13, 2021.

New data points include:

- **Windows PowerShell Log**: PowerShell logs internal operations from the engine, providers, and cmdlets to the Windows event log.
- **Windows PowerShell Operational Log**: Adlumin will support full-script block logging. By default, PowerShell does not leave many artifacts of its execution in most Windows environments. The combination of impressive functionality and stealth has made attacks leveraging PowerShell a nightmare for enterprise security teams.
- **WinRM Logging**: WinRM is a powerful remoting capability used by administrators and attackers. Windows Remote Management (WinRM) is the Microsoft implementation of WS-Management Protocol, a standard Simple Object Access Protocol (SOAP)-based, firewall-friendly protocol that allows hardware and operating ystems from different vendors to interoperate.
- **WMI Logging**: Utilizing WMI in attacks is popular since it does not log much, and is very good for remote attacks, and includes a database to hide persistence and payloads. Adlumin will facilitate the tracking of WMI logs.