**Incident Report:** CH-15143-Defensive-Powershell-Script-Analysis

**Date:** 10-27-2022

**Executive Summary:**

Analyze the Powershell script contained in the file HDWallpaperEngine.txt.

**Script Details:**

* SHA 256 hash value: 0c56591cb8a45b024735b86860b03ec32c0f257644ab0bc360dbbafbb687ef31
* Email account used in execution: [chaudhariparth454@gmail.com](mailto:chaudhariparth454@gmail.com)
* Email account password: yjghfdafsd5464562!
* SMTP Port: 587
* Imported DLL: user32.dll
* Folder where .txt file is stored: temp

**Script Summary:**

This malicious script imports keyboard methods (i.e. GetAsyncKeyState, GetKeyboardState, MapVirtualKey) from user32.dll and uses them to monitor keyboard activity. Upon its execution, the script starts an endless loop that continuously reads the keyboard state, sniffing out the keys that are pressed by the user. When the loop is stopped (CTRL+ C), the recorded keys are logged in a notepad++ .txt. file, which is then sent to the identified email address at the start of the script.