

Ducky Scripts in Powershell

By Zach Riback



The Script – dropfile.ps1

This is just a simple script that is meant to drop a file on the desktop of the current user. It could be used by a rubber ducky to provide proof that the ducky has had access to that computer.

The script can easily be run from the command prompt by typing “Powershell.exe dropfile.ps1 [number of files] [message]”. The number of files argument is the number of text files that the script will drop on the desktop of the user and the message field is the message that will be contained in those files. For instance, running “dropfile.ps1 5 Hello_World” will create 5 files on the desktop each containing the message “Hello_World”.

How it Works

The script first finds the the file path for the desktop which is different for each user. It does this in a way where the script should work for any user. It then reads in a value for \$NumFiles and \$Message from the command line arguments. A for loop is then used to create a new file \$NumFile amount of times, each time with a new name in order to differentiate the files from each other. The files are also creating with the \$Message written to them. This is the entire script, and it serves to show how simple something like this is for a rubber ducky to perform in an environment where the goal is to simply prove that a pentration tester was on the system.