B22 A Baseline for XP Boot Changes

Benjamin R. Livelsberger, BA, National Institute of Standards & Technology, 100 Bureau Drive Stop 8970, Gaithersburg, MD 20899-8970*

After attending this presentation, attendees will become familiar with a baseline of what changes take place to the volumes of a Windows XP system on boot.

This presentation will impact the forensic science community by discussing how an accidental boot to a computer's host operating system is a serious error for a forensic investigator, but understanding the changes that occur when a system boots can mitigate resulting damage.

The behavior of the Windows XP SP2 operating system installed to a FAT32 volume was studied. The operating system was installed and the research was done in an isolated environment. No additional programs were installed, but "user files" were copied to two secondary volumes. Over the course of five boot cycles, before and after images were made of the system. The images were then compared for differing sectors and differences were analyzed using the Sleuth Kit digital investigation tools.

Over the course of five boots and shutdowns of a generic Windows XP system little or no change was made to the secondary volumes, but an average of close to 13,900 sectors changed on the system's boot volume. Changes occurred in each of the boot volume's reserved, FAT, and data areas. On each cycle the reserved area's FS Info sector changed and for each cycle between two and five sectors of the FAT 0 table and between two and five sectors of the FAT1 table changed.

Between 12,501 and 14,827 sectors changed in the data area on each boot. Most of these sectors represented changes to allocated file content. On average, the content of 34 system files changed with the range being 32 - 36 files. A core set of 31 files had content change in each of the five boot cycles. 96% of the changes to file content were to the PAGEFILE.SYS and SYSTEM files (the page file size was 2GB). In general, sectors weren't de-allocated, but on each boot a small number of previously unallocated sectors (averaging around 170, but ranging from 20 to 633) did become allocated.

In the boot volume's data area, in addition to changes to file content and to allocation status, a small number of sectors containing directory entries (file metadata) differed after each boot cycle. For one of the boot cycles, the access times for 497 entries changed, but for the remaining four cycles no access times were altered. Changes to write date and time values were more consistent. On average 54 directory entries had their write date and time values updated with a range of 52 to 55 directory entries. A core set of 51 of those directory entries changed consistently in each of the five boot cycles. Four to seven entries consistently had their size values changed. A set of four of these entries had their size values altered in every cycle and on each cycle eight new directory entries were created.

Having an understanding of the nature of how a system changes on boot and having a baseline for those changes allows the investigator to begin and to defend the examination of an inadvertently booted system.

Boot, Filesystem, FAT32

 ** Presenting Author*