Instalog

Instalog is a senior project proposal by Jacob Snyder (jrs213) and Billy O'Neal (bro4).

At a high level, Instalog is a tool designed to gather as much information from a Windows machine as can feasibly be put into a small, readable log report. Such tools are commonly used for remote support, particularly for removing malicious software from people's machines. In some respects, one might consider this a solved problem. Several tools to accomplish this already exist, such as:

- TrendMicro's *Hijack This*
- "sUBs" *Doesn't Do Squat* (DDS)
- "random/random"'s *Random's System Information Tool* (RSIT)
- "OldTimer"'s *OTL* (Formerly OTListIt)
- "OldTimer"'s *OTS* and *OTA* pair (Formerly OTScanIt and OTAnalyzeIt)

However, these tools all have serious problems, which we believe we can fix in a similar tool:

- Incorrect handling of some types of user data
- Ambiguous report formats that easily lead to machine destroying mistakes
- No published specifications
- No, or extremely buggy/complicated user interfaces
- Slow log generation
- No open source implementations available
- Outstanding bugs that their authors are unwilling or unable to fix
- No scriptability
- Lack of 64-bit support

We can't entirely fault these other tools for having deficiencies. Tools of this variety are quite complex due to the many different loading points that these tools report. We think that by creating a tool that is open-source, it will be easier for the community and us to address bugs. This would be the first tool of its nature that is open-source.

Moreover, the similar tools available are designed to help the remote administrator or the local administrator, but make design compromises that make operating on a system cumbersome for one or the other. We believe we can fix these problems and produce a tool that is more safe, more scalable, more preferment, and easier to use than similar tools currently available.

We have conducted surveys of forums which commonly use similar logging tools, and have support from their staff for beta testing. If we have a user base similar to our "spiritual predecessor" DDS, that will be *tens of thousands* of computers, running *hundreds of thousands* of pieces of malware, *per month*.