

Indications of System Compromise

April 2017

BJ Bellamy

The purpose of this paper is to provide actionable information that can assist in identifying potential malicious (unauthorized, adversarial, or mistaken) system compromise.

End users of server and other infrastructure systems are far enough removed from the servers they use that unless there is a tangible interruption or slow-down of services they are unaware of the operational or security status of these hosts that they rely on.

Excessive and/or unusual:

- CPU utilization
- use of disk space
- disk activity regardless of the amount of free space
- network activity or errors
- Recently installed software
- Errors in the Windows event logs
- Errors in the *nix dmesg log
- Unexpected reboots
- Problems that seem to require a reboot
- Unauthorized or unusual access to resources, or the failed attempt

An idea is to develop benchmarks that can be checked to determine if a system is behaving as usual. This could include a graph of the event logs error messages, comparisons of used disk space use and IO, CPU utilization, and network statistics to previous “norms”. This type of information may already be captured for other purposes and could be re-tasked.