

TABLE OF EVIDENCE

EVIDENCE ID	001
SOURCE	RAM Dump
FINDINGS	Process <code>svchost.exe</code> (PID 4022) contained an unbacked memory section with an "MZ" header (Malware).