CounterTack | ManTech Cyber Solutions International

Responder® PRO
Powered by Digital DNA®

CounterTack Responder® PRO

Physical Memory Forensics and Malware Analysis

Responder® PRO, the defacto industry standard for Windows physical memory acquisition and analysis, is now also available for Linux. With its unparalleled memory forensics and behavioral analysis capabilities, Responder PRO cuts through the wide array of anti-forensic measures employed by today's most stealthy malware, and uncovers artifacts critical for incident response, data compliance and electronic discovery. Cyber Security Analysts can now pull in and analyze both Windows® and Linux memory images to perform memory forensics on endpoints.

LIVE MEMORY ACQUISITION AND ANALYSIS

Responder PRO includes FastDump™ PRO, a comprehensive memory acquisition tool that supports full capturing of Windows and Linux physical and virtual memory (both RAM and paging file). FastDump PRO performs fast, accurate, forensically sound memory imaging. Once captured memory is analyzed, Responder PRO makes it easy to search, identify, and report on critical digital artifacts like passwords, encryption keys, Internet search histories, and other forensic data.

Generate fast, actionable threat intelligence about methods of infection, files and registry keys accessed, networking behaviors, and more.

Responder PRO's intuitive interface integrates smoothly with existing tools and processes to streamline your investigative workflow and produce rapid results.

Automatically reverse engineer and analyze physical memory to reveal zero-day malware, rootkits, and other hard-to-detect threats.

MALWARE DETECTION MADE EASY WITH DIGITAL DNA®

When you add Digital DNA®, CounterTack's patented memory analysis technology, Responder PRO automatically reverse engineers memory images and examines it for potentially malicious capabilities. Observed behavioral traits are matched against CounterTack's Malware Genome database to classify digital objects as good, bad or neutral. Rules and weighting are applied to compute the overall severity score, which is presented as part of a comprehensive threat profile.

TYPES OF INFORMATION FOUND IN LIVE MEMORY

Operating system information:

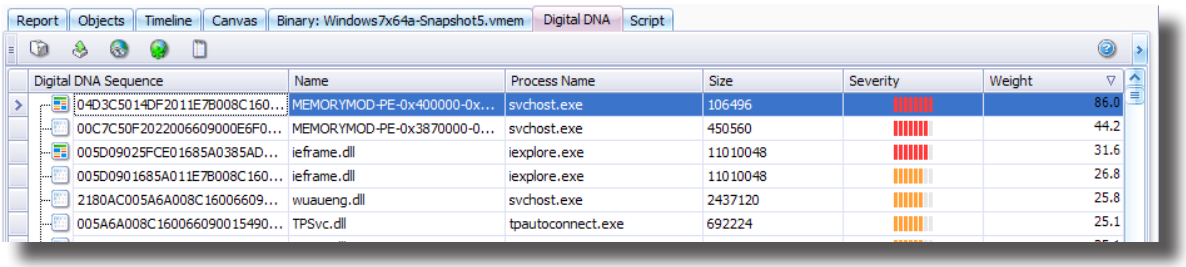
- Running processes and modules
- Open files
- Network connections and listening port
- Open registry keys
- Interrupt Descriptor Table
- System Services Descriptor Table

Application information:

- Password in clear text
- Unencrypted data
- Instant messanger chat sessions
- Document data
- Web-based email
- Outlook email

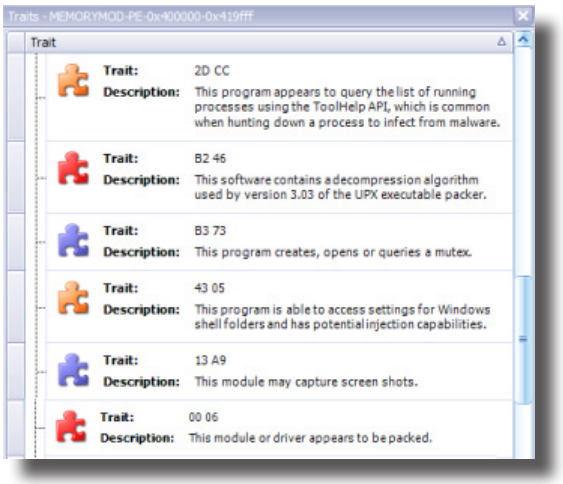
Malware Detection:

- Keystroke loggers
- Rootkits
- Trojans
- Bots
- Banking Trojans
- Polymorphic code



The Netwire RAT exhibits suspicious behaviors that cause Digital DNA to flag it as a threat.

A separate Traits panel drills down into specific behaviors and gives you fast insight into the unique combinations of tools and techniques favored by individual attackers and groups.



By attempting to disguise itself, the Netwire RAT makes itself appear even more suspicious to Digital DNA.

GRAPHING AND REPORTING

The Responder PRO Canvas view provides an interactive graphical window of the elements that make up a piece of malware and how they link to other parts of the system. Canvas graphs offer a tangible model for tracing program behaviors by allowing you to traverse, isolate or connect branches of execution, collapse and expand functions, and jump directly to relevant sections of disassembly and raw data in the Binary view.

A function that locates an embedded module and loads it into memory. Digital DNA will flag the module as suspicious if it is packed or exhibits other behaviors common to malware.

The Report view presents short, comprehensive text summaries of suspicious binaries identifed by the Responder PRO's built in automated malware analysis tools. Designed for ease of use, Responder PRO reports provide critical threat intelligence at a glance.

Conduct forensically sound digital investigations and produce concise, accurate reports for management, law enforcement and other stakeholders.

Installation Requirements

- Mircosoft Windows Server 2008/2012

OR

- Microsoft Windows 7 & 8.1 (64-bit)
- Minimum 4GB RAM

Physical Memory OS Compatibility

The new Responder PRO covers the two most popular versions of Linux available today, Red Hat Enterprise Linux (RHEL) 6 & 7 and CentOS 6 & 7 in addition to Windows XP, Vista, 7, 8, 8.1, Windows Server 2008 & 2012 (including R2).

CounterTack | ManTech Cyber Solutions International

100 5th Ave, First Floor
Waltham, MA 02451-1208
855.893.5428
www.countertack.com