HBGary
Detecting Tomorrow's Threats Today
ManTech International Corporation

RESPONDER™ PROFESSIONAL
for Digital Forensics

Responder™ Pro is the de facto industry standard for Windows® physical memory acquisition and analysis. 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. Its intuitive interface also integrates smoothly with existing tools and processes to streamline your investigative workflow and produce rapid results.

Generate fast, actionable **THREAT INTELLIGENCE** about **METHODS OF INFECTION**, **FILES** and **REGISTRY KEYS** accessed, **NETWORKING** behaviors, and more.

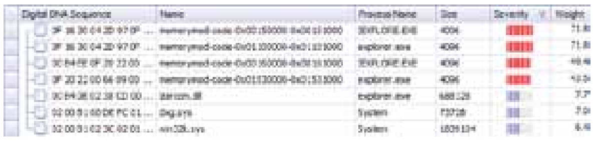
Live MEMORY ACQUISITION and ANALYSIS

Responder™ Pro includes FastDump™ Pro, a comprehensive memory acquisition tool that supports full capturing of Windows® 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.

Automatically **REVERSE ENGINEER** and analyze physical memory to reveal **ZERO-DAY malware**, **ROOTKITS**, and other hard-to-detect threats.

Malware DETECTION with DIGITAL DNA

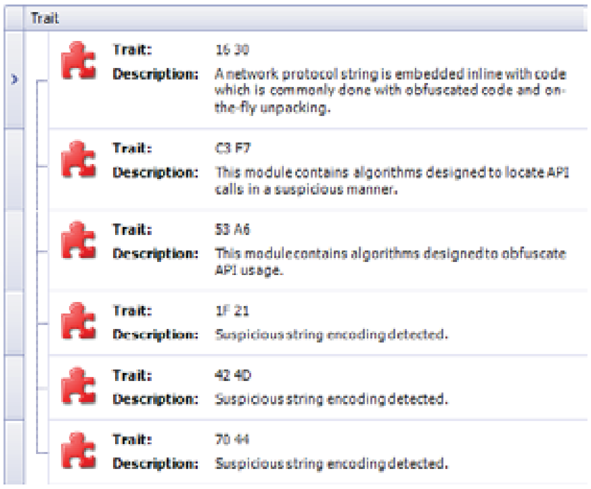
Using Digital DNA™, HBGary's revolutionary memory analysis technology, Responder™ Pro automatically reverse engineers all code in memory and examines it for potentially malicious capabilities. Observed behavioral traits are matched against HBGary's Malware Genome database to classify digital objects 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. Digital DNA is a yearly subscription add-on to Responder™ Pro.



Digital DNA Sequence	Name	Process Name	Size	Severity	Weight
3F 16 30 04 20 97 0F ...	memorymod-code-0x00150000-0x00151000	IEXPLORE.EXE	4096	🟥	71.8
3F 16 30 04 20 97 0F ...	memorymod-code-0x01100000-0x01101000	explorer.exe	4096	🟥	71.8
3C 84 FE 0F 39 22 00 ...	[illegible]	IEXPLORE.EXE	4096	🟥	[illegible]
3F 20 22 00 66 09 00 ...	[illegible]	explorer.exe	4096	🟥	[illegible]
3C 84 2B 02 38 CD 00 ...	[illegible]	explorer.exe	688128	🟦	7.7
02 00 31 60 0E FC C1 ...	[illegible]	System	73728	🟦	7.0
02 00 31 02 3C 02 01 ...	win32k.sys	System	[illegible]	🟦	[illegible]

[The Poison Ivy Trojan 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.



Trait

Trait: 16 30
Description: A network protocol string is embedded inline with code which is commonly done with obfuscated code and on-the-fly unpacking.

Trait: C3 F7
Description: This module contains algorithms designed to locate API calls in a suspicious manner.

Trait: 53 A6
Description: This module contains algorithms designed to obfuscate API usage.

Trait: 1F 21
Description: Suspicious string encoding detected.

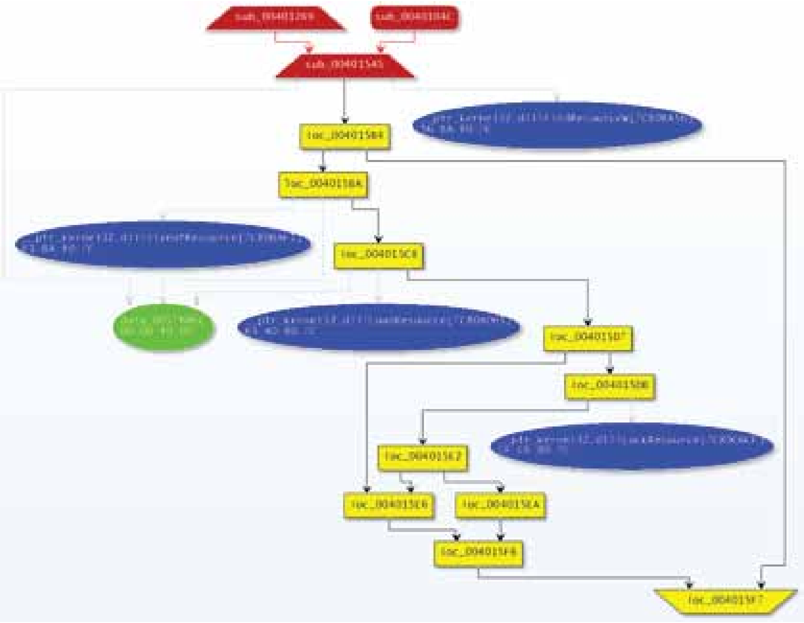
Trait: 42 4D
Description: Suspicious string encoding detected.

Trait: 70 44
Description: Suspicious string encoding detected.

[By attempting to disguise its capabilities, Poison Ivy 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 identified by the Responder™ Pro automated Malware Analysis tools. Designed for ease of use, Responder™ Pro reports provide critical threat intelligence at a glance.

Scan me now

- Obtain more information about HBGary's Responder™ Professional.
- View demonstrations online

Types of INFORMATION found in LIVE MEMORY

Operating system information

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

Application information

- Passwords in clear text
- Unencrypted data
- Instant messenger chat sessions
- Document data
- Web-based email
- Outlook email

Malware Detection

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

Conduct **FORENSICALLY sound** digital **INVESTIGATIONS** and produce concise, accurate reports for **MANAGEMENT, LAW ENFORCEMENT** and other non-experts.

System Requirements

- Microsoft Windows XP (with Service Pack 2+)
- Microsoft Windows Server 2003/2008 (Vista)
- Microsoft Windows 7 32-bit and 64-bit
- Minimum 1 GB of RAM (2GB recommended)
- Minimum 150 MB of available hard disk drive space.