CounterTack®

CounterTack Digital DNA®

Technology Brief

Digital DNA® is the only deep behavioral analysis technology that forensically analyzes an endpoint's memory to detect the most advanced threats, including those used against global organizations for theft of intellectual property, classified information and customer records.

THE POWER OF DIGITAL DNA

With its unparalleled memory forensics, our patented DNA technology cuts through the wide array of anti-forensic measures employed by today's most stealthy malware. Once a threat has been identified, automated analysis provides fast insight into its capabilities and empowers you to pinpoint other potentially compromised systems, determine initial points of infection, and isolate lingering malicious files and system changes.

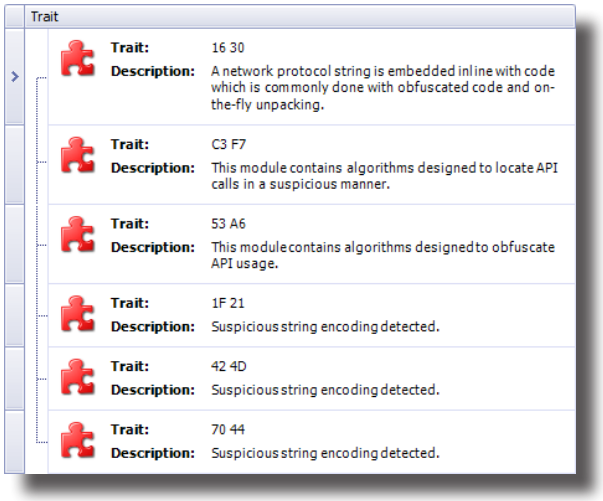
COUNTERTACK'S DIGITAL DNA TECHNOLOGY LICENSING PROGRAM

If you are an existing security vendor, hardware manufacturer, software provider, or cloud-based solution company, CounterTack is now offering Digital DNA® (DDNA) the only patented memory analysis technology that automatically reverse engineers memory images and examines code for potentially malicious behavioral traits & threats. You can easily integrate Digital DNA technology (software development kit: driver, API, and library) into your product or service and offer immediate a value-added security service to your customers.

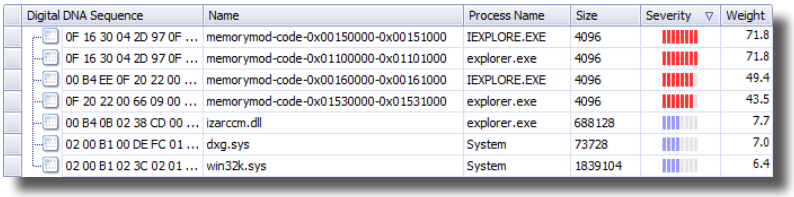
HOW IT WORKS

Digital DNA automatically reverse engineers all code in memory and maps each module's capabilities at the lowest level to determine if it behaves like malware - without relying on signatures, IOCS or heuristics. Behaviors are matched against traits from CounterTack's Malware Genome database and classified as good, bad, or neutral. Rules and weighting are applied to compute the module's overall severity score, which is presented as part of a comprehensive threat profile.

By accessing physical memory directly and identifying the specific behavioral traits of each module, Digital DNA reliably detects the vast quantities of new malware that signature based methods miss, including zero-days, root kits, and targeted attacks.



The Traits sequence provides actionable intelligence about methods of infection, files and registry keys accessed, networking behaviors, and more.



Digital DNA Sequence	Name	Process Name	Size	Severity	Weight
0F 16 30 04 2D 97 0F ...	memorymod-code-0x00150000-0x00151000	IEXPLORE.EXE	4096		71.8
0F 16 30 04 2D 97 0F ...	memorymod-code-0x01100000-0x01101000	explorer.exe	4096		71.8
00 B4 EE 0F 20 22 00 ...	memorymod-code-0x00160000-0x00161000	IEXPLORE.EXE	4096		49.4
0F 20 22 00 66 09 00 ...	memorymod-code-0x01530000-0x01531000	explorer.exe	4096		43.5
00 B4 0B 02 38 CD 00 ...	izarccm.dll	explorer.exe	688128		7.7
02 00 B1 00 DE FC 01 ...	dxg.sys	System	73728		7.0
02 00 B1 02 3C 02 01 ...	win32k.sys	System	1839104		6.4

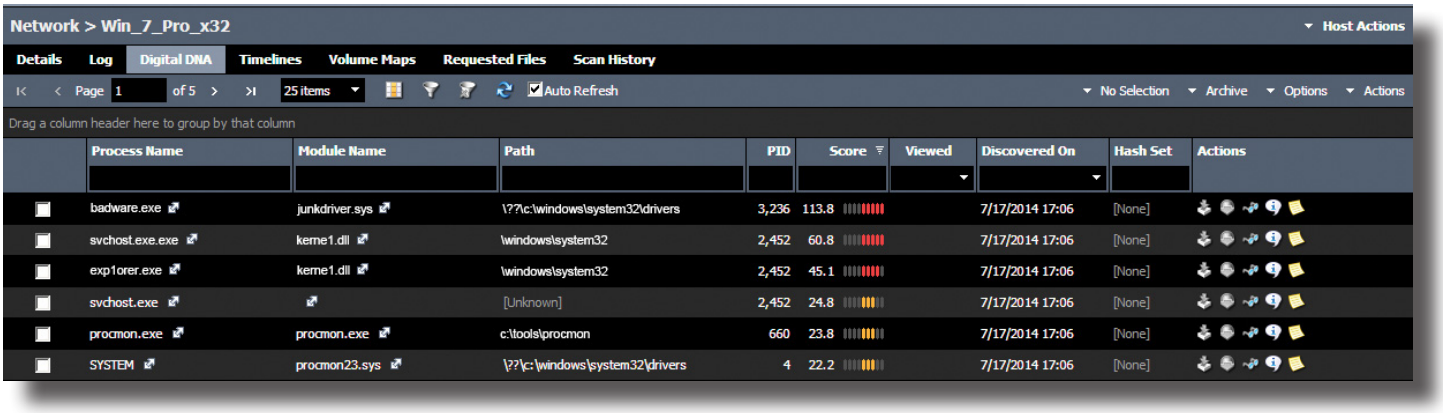
Digital DNA's intuitive, color-coded interface provides at-a-glance risk assessment.

EFFICACY TESTING

CounterTack conducts continuous efficacy testing of Digital DNA to ensure successful detection of never-before-seen threats. For each round of testing, 25,000 malicious binaries are selected randomly from third-party feeds and scanned. Digital DNA currently has a positive detection rate of 93% for unknown threats.

DIGITAL DNA FOR COUNTERTACK's ACTIVE DEFENSE™

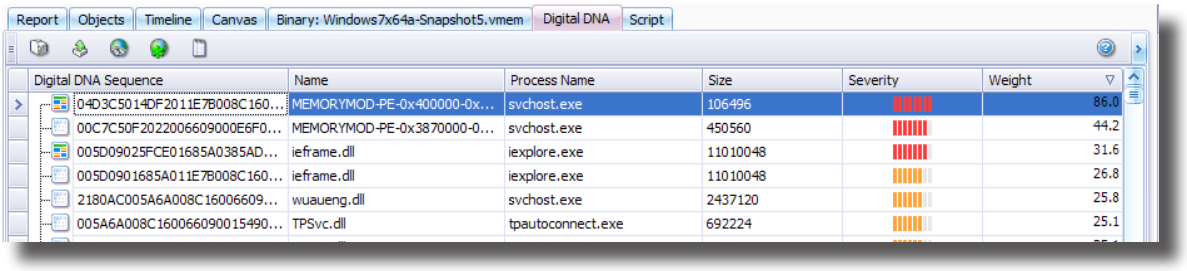
Active Defense is an enterprise-wide Digital DNA management solution that allows you to scan raw physical memory, the live operating system, and NTFS volumes from a central console. Once a threat has been identified, automated collection and analysis capabilities streamline the incident response lifecycle, allowing your team to scale its efforts to tens or hundreds of thousands of systems - without requiring armies of highly skilled analysts.



Active Defense, powered by Digital DNA technology, forensically scans a snapshot of endpoint memory and uses Digital DNA to rate threat severity of executable code.

DIGITAL DNA FOR COUNTERTACK's RESPONDER® PRO

Responder PRO is the defacto industry standard for Windows® and Linux physical memory acquisition and analysis. In just a few clicks, Responder PRO detects malware in live memory, enumerates its capabilities, and uncovers artifacts critical for incident response, data compliance, and electronic discovery. With Responder PRO, your incident response team can easily understand any cyber threat and quickly reinforce network defenses against it.



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

CounterTack®

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