

DIGITAL DNA

Breakthrough Malware Detection System

Enterprises must reduce the risk of cyber threats to protect critical data and operational assets. Intellectual property, confidential information, trade secrets, financial data, and money are being stolen at increasing rates. New malicious code is introduced daily into networks through the Internet and insider threats. Studies prove that commercial anti-virus and traditional host intrusion detection systems don't detect 80% of new malware, especially new variants, polymorphic code, and malware that resides only in memory or hides using rootkits.




Digital DNA is a revolutionary technology to detect advanced computer security threats within physical memory without relying on the Windows operating system which cannot be trusted. All software modules residing in memory are identified and ranked by level of Severity. The Digital DNA Sequence appears as a series of Trait code---s when concatenated together describe the behaviors of each software module.

The screenshots below show threat Severity and a partial list of Traits related to an example module called iimo.sys.

Ranking Software Modules by Threat Severity using Digital

Digital DNA Sequence	Module	Process	Severity	Weight
0B 8A C2 05 0F 51 03 0F 6...	iimo.sys	System	■■■■■	92.7
0B 8A C2 02 21 3D 00 08 63	ipfltdrv.sys	System	■■■■	13.0
0B 8A C2	intelpm.sys	System	■■■■	11.0
05 19 34 2F 57 42 00 7E 1...	ks.sys	System	■■■■	-10.0
02 21 3D 2F 1C FD 00 08 63	ipnat.sys	System	■■■■	-13.0
2F 7B ED	ipsec.sys	System	■■■■	-15.0

Software Behavioral Traits

Trait	
	<p>Trait: 8A C2</p> <p>Description: The driver may be a rootkit or anti-rootkit tool. It should be examined in more detail.</p>
	<p>Trait: 0F 51</p> <p>Description: There is a small indicator that detour patching could be supported by this software package. Detour patching is a known malware technique and is also used by some hacking programs and system utilities.</p>
	<p>Trait: 0F 64</p> <p>Description: The driver has a potential hook point onto the windows TCP stack. This is common to desktop firewalls and also a known rootkit technique.</p>

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. Users can see the underlying Trait descriptions to gain fast insight into software behaviors.

Ultimately, any network can and will be compromised. Digital DNA is your last line of defense in a defense-in-depth strategy. Reduce risk by quickly detecting new threats that are bypassing your existing security infrastructure.

