The Most Powerful Weapon Against Targeted Attacks

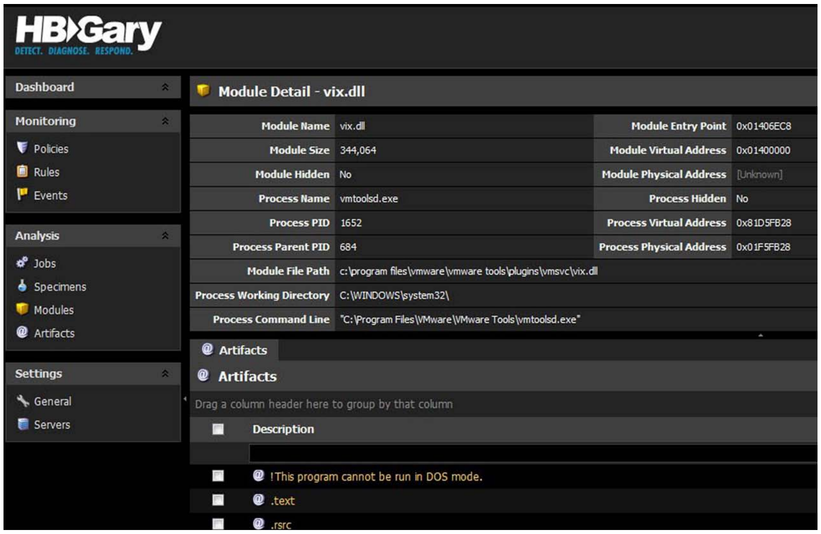
Perimeter security and some behavior-based solutions built on sandboxing and other outdated methodology can't detect all unknown threats. You need a proven solution that detects, without signatures, targeted malware and other unknown threats, in the one place where it can't hide – physical memory. Protect your organization with the most advanced perimeter weapon available against targeted attacks – Razor™.

Leveraging HBGary's proven core technology, Digital DNA™, Razor uses a non-signature, behavior-based methodology that detects unknown threats using physical memory. Razor captures all executable code within the Windows® operating system, and running programs that can be found in physical memory, including targeted attacks, rootkits, injected code and custom malware so organizations can provide near real-time response.

Built on HBGary's innovative, proven technology to detect targeted attacks at the host, Razor provides both perimeter- and host-level threat information to create the industry's most comprehensive threat intelligence available today.

Razor Performs Behavioral Analysis at the Perimeter

- **Document capture** – Captures documents in real-time passively from the network.
- **File detonation** – 'Detonates' these captured files within a virtual machine where it performs extremely low-level tracing of all instructions. This data is used to recover clear-text information and behaviors that reveal whether the document is malicious.
- **Real-time alerts** – Makes captured information available at the console for the analyst and generates a real-time alert.
- **Command-and-Control protocol analysis and alerting** – Detects known malicious command-and-control using a combination of DNS intelligence, protocol patterns, netblock reputation and country-of-origin data. The ruleset is updated as part of the Digital DNA subscription, and customers can specify custom rules.
- **Block Malicious Traffic** – This optional feature automatically blocks all further traffic associated with the malicious site and/or document. HBGary provides regular updates for the Digital DNA behavioral rule set.



Module Detail - vix.dll

Module Name	vix.dll	Module Entry Point	0x01406EC8
Module Size	344,064	Module Virtual Address	0x01400000
Module Hidden	No	Module Physical Address	[Unknown]
Process Name	vmtoolsd.exe	Process Hidden	No
Process PID	1652	Process Virtual Address	0x81D5FB28
Process Parent PID	684	Process Physical Address	0x01F5FB28
Module File Path	c:\program files\vmware\vmware tools\plugins\vmsvc\vix.dll		
Process Working Directory	C:\WINDOWS\system32\		
Process Command Line	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"		

Artifacts

Artifacts

Drag a column header here to group by that column

□	Description
□	!This program cannot be run in DOS mode.
□	.text
□	.rsrc

Technical Requirements

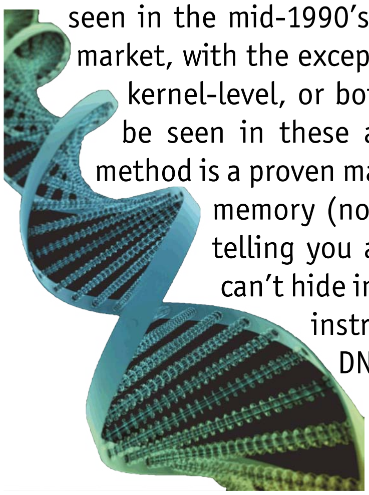
- Razor sniffs network data up to 50 Mb/s (DS3)
- Packaged and shipped as an server-based appliance
- Web-based console management requires Internet Explorer 7.0 or equivalent

Razor Appliance Specifications

- Windows Server 2008 R2 64-bit 5-user operating system
- Intel Xeon X3430 2.4 8MB Tray Quad Core 1156
- 2GB PC3-10667 ECC Unbuffered STD DDR3 1333 Micron
- Two Seagate Constellation ES 1TB SATA 3.0 7200 32MB 3.5in
- Dual Intel® 82574L Gigabit Ethernet Controllers
- Adaptec RAID 2405 4-Port PCI-E SAS/SATA RAID Controller Card
- Matrox G200eW 16MB DDR2

HBGary
DEFEATING TOMORROW'S MALWARE TODAY
3604 Fair Oaks Blvd
Suite 250
Sacramento, CA 95864
Phone: 916-459-4727
http://www.hbgary.com

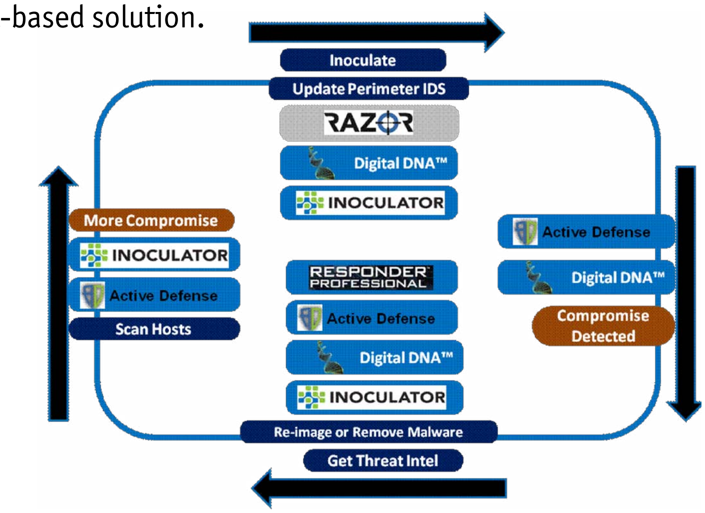
HBGary Digital DNA vs. Behavior-based Sandboxes



All sandboxes are not created equally. In fact, some of the earliest sandboxes seen in the mid-1990's are still in use today. All sandboxes on the market, with the exception of Razor, monitor activity at the user- or kernel-level, or both, yet malware easily manipulates what can be seen in these areas. HBGary's Digital DNA behavior-based method is a proven malware detection approach that scans physical memory (not virtual, which is just the operating system telling you about itself). Rootkits and targeted malware can't hide in physical memory – a correct set of execution instructions is needed or it will not run. Digital DNA is the only solution that provides accurate behavior information, which increases the effectiveness of detecting malware, and correctly identify malicious code.

HBGary's Continuous Protection Product Suite

HBGary's Continuous Protection product suite, with its flagship product Active Defense, provides host-level and perimeter-level protection critical to protect data, transactions and intellectual property. By monitoring physical memory, raw disk, and live operating systems across the Enterprise, HBGary provides an unprecedented view of known and unknown threats. This threat intelligence can continuously be updated to your existing security infrastructure to mitigate risk – eliminating need for expensive forensics and reducing cost/time required for incident response. HBGary's Continuous Protection product suite includes Razor, Inoculator™, Active Defense™, HBGary Responder™ and Digital DNA. Razor is HBGary's first network-based solution.


Inoculate
Update Perimeter IDS
RAZOR
Digital DNA™
INOCULATOR
More Compromise
INOCULATOR
Active Defense
Scan Hosts
RESPONDER PROFESSIONAL
Active Defense
Digital DNA™
INOCULATOR
Active Defense
Digital DNA™
Compromise Detected
Re-image or Remove Malware
Get Threat Intel