

# RAZOR

## 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Perimeter security and some behavior-based solutions built on sandboxing and other outdated methodology can't detect all unknown threats.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	vmttoolsd.exe	Process Hidden	No
Process PID	1652	Process Virtual Address	0x81D5F828
Process Parent PID	684	Process Physical Address	0x01F5FB28
Module File Path	c:\program files\vmware\vmware tools\plugins\vmtoolsd\plugins\vix.dll		
Process Working Directory	C:\WINDOWS\system32\		
Process Command Line	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"		
<b>Artifacts</b>			
Drag a column header here to group by that column			
<b>Description</b>			
<input type="checkbox"/>	! This program cannot be run in DOS mode.		
<input type="checkbox"/>	.text		
<input type="checkbox"/>	.rsrc		

