From: "Jim Moore" <jim@jmoorepartners.com>
To: "Greg Hoglund" <greg@hbgary.com>
Sent: Tuesday, October 19, 2010 4:27 PM
Attach: HBGARY.pptx; HBGary CIM.pdf
Subject: FW: Analyst slide deck and IM

James A. Moore
J. Moore Partners
Mergers & Acquisitions for Technology Companies
Office (415) 466-3410
Cell (415) 515-1271
Fax (415) 466-3402
311 California St, Suite 400
San Francisco, CA 94104
www.jmoorepartners.com

From: Jim Moore
Sent: Monday, October 18, 2010 11:03 AM
To: 'ken_gonzalez@mcafee.com'
Cc: Matthew Droessler
Subject: Analyst slide deck and IM

Ken,

Good to speak with you on Friday. As discussed, management has retained us to field the many inquiries they are receiving and to help them evaluate the various options. Attached are the analyst slide deck and an IM for your internal use. We see several ways in which this technology could take the McAfee offering to the next level, below is a short list.

1. Allows McAfee to up sell a solution designed to deal with APT.
2. DDNA with Responder Pro allows McAfee to more quickly produce a signature with less effort than existing solutions.
3. HBGary is addressing the top two issues in government agencies; the ability to respond to cyber attacks and detect them . One immediate advantage is that this makes McAfee more competitive for the re-bid of HBSS.
4. This gives McAfee two areas of immediate growth in managed services. First is the ability to do a more comprehensive engagement; DDNA will find known and unknown malware. Therefore, if it's known and the AV or IDS should have picked it up, then there is an engagement to help solidify the client's infrastructure. If it's unknown then it is an APT engagement. More machines, less time. If in fact new items are discovered, McAfee can up sell a managed service looking for APT (this is the PwC model).
5. While it isn't announced yet, HB Gary will have an Inoculator product which will allow antibodies to be installed so that a known malware cannot re-install.

Since we are on a fast track here due to the interest level and intensity, I would like to work with you to set up the management meeting in the next couple of weeks. Would the 25th, 26th, 29th, or 2nd work?

Kind regards,

Jim

James A. Moore
J. Moore Partners
Mergers & Acquisitions for Technology Companies
Office (415) 466-3410

Cell (415) 515-1271
Fax (415) 466-3402
311 California St, Suite 400
San Francisco, CA 94104
www.jmoorepartners.com

HBGary

DEFEATING TOMORROW'S THREAT TODAY

Confidential Information Memorandum

J.MOORE

PARTNERS

MERGERS & ACQUISITIONS
FOR TECHNOLOGY COMPANIES

Table of Contents

Executive Summary

Since its founding in 2004, HBGary, Inc. has developed risk mitigation solutions to identify unknown malware, decrease the time and costs associated with incident response, and facilitate the process in convicting cybercriminals. ***Solutions from this innovative security software firm allow its customers to rapidly assess, diagnose, and respond to exceptionally advanced attack technologies.***

Gartner

"For several years, the most damaging attacks have used targeted custom malware that evades traditional anti-virus and Web security gateway controls. ***HBGary provides a set of products for analyzing executables and system configurations to detect, inspect and analyze advanced malware, based on its patent-pending Digital DNA technology."***

Source: Gartner Research, April 2010

Industry Overview

The accelerating prevalence of the World Wide Web has powered the unprecedented expansion of information technology. Because of this paradigm shift in information storage, organizations now hold their most valuable assets in virtualized or digitized environments. Unfortunately, this transformation has resulted in largely insecure information systems that are vulnerable to exploitation by highly motivated and sophisticated cyber-spies and digital criminals. Intellectual property such as product designs, marketing plans, customer lists, and government assets are being stolen at an increasing rate.

McAfee

"Businesses lose more than $1 trillion in Intellectual property due to data theft and cybercrime."

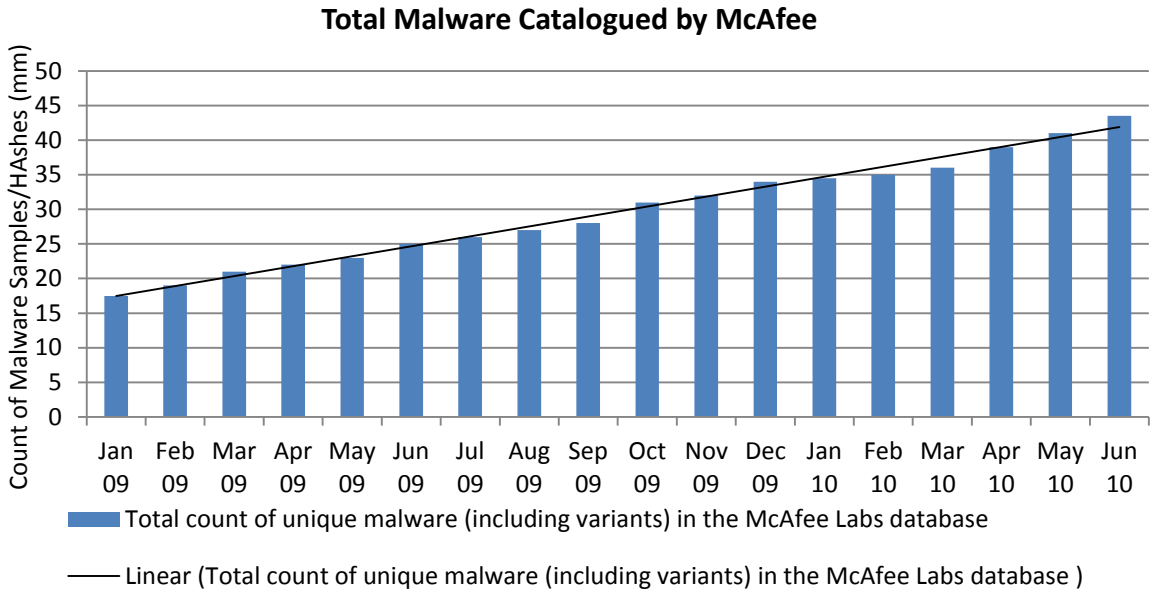
Source: McAfee, 2009

To date, entities stand to lose more from a data breach than ever before. Based on a 2009 study performed by researchers from Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS), McAfee estimates that companies worldwide lost more than $1 trillion in 2009 from cyber attacks.[1] The report, *Unsecured Economies: Protecting Vital Information,* examined responses from more than 800 CIOs in the United States, the United Kingdom, Germany, Japan, China, India, Brazil and Dubai. The companies surveyed estimated their combined losses of intellectual property to be $4.6 billion over the last year alone, while spending approximately $600 million repairing damages from the data breaches.[2] Due to the high cost of compromised intellectual property, organizations must allocate significant capital towards progressive defense technologies as malware becomes more ubiquitous.

[1] McAfee, January 2009

[2] The Center for Education and Research in Information Assurance and Security, *Unsecured Economies: Protecting Vital Information,* January 2009

The graph below indicates the total volume of malware detected by McAfee on a per month basis. As of June 2010, McAfee has catalogued a total of over 40 million different types of malware. Most notable, McAfee has cataloged *10 million* new pieces of malware in the first half of 2010, making this period the most active half-year ever for total malware productions. During the same period in 2009, McAfee discovered 9 million new pieces of malware.[10] Additionally, during 2009, PandaLabs, the anti-malware lab of Panda Security, identified 25 million new malware samples.[3] Prior to 2009, the Company had identified a total of 15 million pieces of malware in 19 years.



Traditional security software solutions are not providing sufficient defense against today's cyber threats. Existing IT security investments such as endpoint anti-malware, intrusion detection and firewalls are necessary, but inadequate in protecting enterprise data.[9] These solutions fail because they do not have prior knowledge of the threat, do not understand the malicious behavior of malware, cannot scale with the sophistication and volume of modern malware, and do not secure the end node thereby exposing digital assets to an infinite number of threats.

Company

HBGary, Inc. was founded in 2004 to counter advanced foreign intelligence threats penetrating Department of Defense (DoD) computer networks. Initially, the Company's works were offensive in nature but, shortly thereafter, HBGary leveraged their expertise in attack software to develop cutting-edge malware defense products. Founder, renowned security expert Greg Hoglund, understood that advanced threats were evolving faster than current security measures and this would result in more security breaches that organizations were ill equipped to handle.

By focusing on end node advanced, behavior-based malware detection and the monitoring of physical memory (RAM), HBGary has revolutionized the way in which enterprises combat malicious cyber attacks and protect digital assets. The United States Air Force and Department of Homeland Security

[3] PandaLabs Annual Report, December 2009

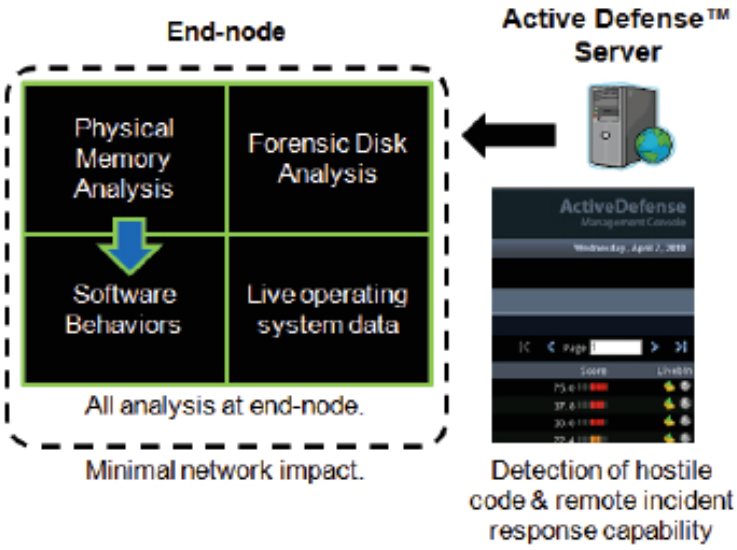
understood HBGary's strengths and shared this vision of the problem, ultimately awarding HBGary multiple grants to develop advanced reverse engineering and threat detection technologies, which also facilitated the understanding of malware from a new and innovative perspective. Since then, HBGary has successfully delivered several products that have captured a significant portion of the ballooning 'advanced threats' marketplace.

HBGary's high profile customers include major corporations, government agencies and government contractors. Just a few of their customers are JP Morgan, General Electric, the FBI, the Department of Justice, Boeing and Northrop Grumman.

The Company explores four critical areas to find advanced threats and provides the following analysis:

- analysis based upon behavior traits
- enterprise memory analysis and forensics
- disk analysis and forensics
- live operating system searching

This is all done concurrently in an enterprise framework.



Most of HBGary's competition uses disk-based scanning and operating-system queries to detect malware. Both of these approaches are easily and commonly evaded by modern malware and advanced attackers.

Because these traditional methods have proven to be unsuccessful, HBGary approaches the problem from an innovative perspective. HBGary combines enterprise-wide *physical memory* analysis with patent-pending Digital DNA technology to detect malicious code in execution. HBGary incorporates this superior detection capability with live-forensic features to allow the user to find and diagnose problems proactively before they become critical. Currently, HBGary's solutions cannot be matched across all four categories of support.

Leadership in Threat Detection, Analysis and Diagnosis

HBGary provides best in class security solutions that outperform all existing anti-virus and perimeter security products. The Company's unique product suite offers the most sophisticated threat detection, malware and memory forensics solutions available allowing organizations to quickly gather critical evidence to contain the threat, locate compromised machines, and assess the damage.

the 451 group

"By understanding key elements of Microsoft Windows memory management architecture, ***HBGary has developed tools that can reconstruct captured Windows images (including VMs) with total accuracy and then step through program execution at a granular level, showing memory allocation, library and processor access,*** *etc. – and then use that unique information to fingerprint malware executables, changes linked to malware infection or other activity, and extract forensic information from memory post-infection."*

Source: The 451 Group, March 2010

Centered upon Digital DNA, a signature-less method of detecting malware using behavioral-based malware identities, the Company's technology effectively focuses on the end node by acquiring and analyzing physical memory (RAM) images at the lowest possible level in a 'forensically-sound' manner with full support for Windows 32 and 64 bit platforms. Because HBGary's technology monitors all applications and processes running in memory, the solutions naturally scale to monitor hundreds of thousands of end nodes.

Focusing on the advanced threat space by analyzing, diagnosing, and advising cyber attack victims, HBGary differentiates itself by designing their platform to detect malware that has previously not been identified. This is in contrast to traditional anti-virus solutions that cannot detect brand new malware and can only protect against what they have already detected.

HBGary is the only solution that uses code-logic to determine behavior. All other solutions currently available use only binary indicators that are unrelated to code behavior and, thus, inaccurate in classifying new malicious code traits.

No other vendor in the marketplace offers a comparable solution to HBGary's product suite. This technology is imperative for any organization seeking to bolster its security defense network or for any participant in the security space interested in offering the most complete threat detection software to date.

HBGary's leading product suite includes the following functionality:

- Understands and diagnoses the most evolved malware
- Rapidly understands the common code and forms of attack, immediately leveraging its knowledgebase more effectively to analyze and disable the malware
- Detects zero day malware or targeted malware, through HBGary's code level analysis of software in physical or virtualized memory
- Detects and prioritizes the vast majority of malware in the system based upon the threat levelAcquires and analyzes physical memory (RAM) images at the lowest possible level in a 'forensically sound' manner with full support for Windows 32 and 64 bit platform
- Organically scales to monitor hundreds of thousands of end-nodes by monitoring RAM, rather than relying upon perimeter security solutions
- Detects encrypted malware since encrypted malware decrypts itself and becomes active in RAM
- 'Carves' and reconstructs the operating system state from only physical memory, in both real and virtual environments, providing a higher barrier to entry for potential competitors
- Extracts running binary code and modules from physical memory. This feature defeats packing, polymorphism, hidden hooks and obfuscation, all of which are severe problems for traditional anti-virus and intrusion detection systems
- Recovers code and data from binary executable objects
- Disassembles binary executable objects and reconstructs logic pathways. Scans memory and reconstructed objects for behaviors and symbols to provide the most accurate understanding of the malware characteristics
- Presents human-readable technical information about binary object behaviors
- HBGary is the only company in this space to have full platform coverage with the ability to collect the pagefile and also collect over four gigabytes of RAM

Industry Overview

The development of a global economy has fueled the monumental expansion of information technology. Massively interconnected systems, including the global Internet, deliver information to more people faster than ever. Unfortunately, this transformation has resulted in largely insecure information systems that are vulnerable to exploitation by highly motivated and sophisticated cyber-spies and digital criminals. Intellectual property such as product designs, marketing plans, customer lists, and government assets are being stolen at an increasing rate.

Besides the immense strategic implications resulting from the loss of valuable intellectual property, these cyber attacks result in significant financial losses to the affected organizations. In 2009, PGP Corporation – acquired by Symantec Corporation in June 2010 - released its annual study, Global Cost of a Data Breach, with the following statistics illustrating the damage to the victims of cyber attacks. US organizations reported the highest average total cost per data breach, average cost per compromised record, maximum total cost, and maximum data breach on a per size basis.[4] Globally, the average total cost per data breach for an organization stood at $3.43 million for this past year. [1]

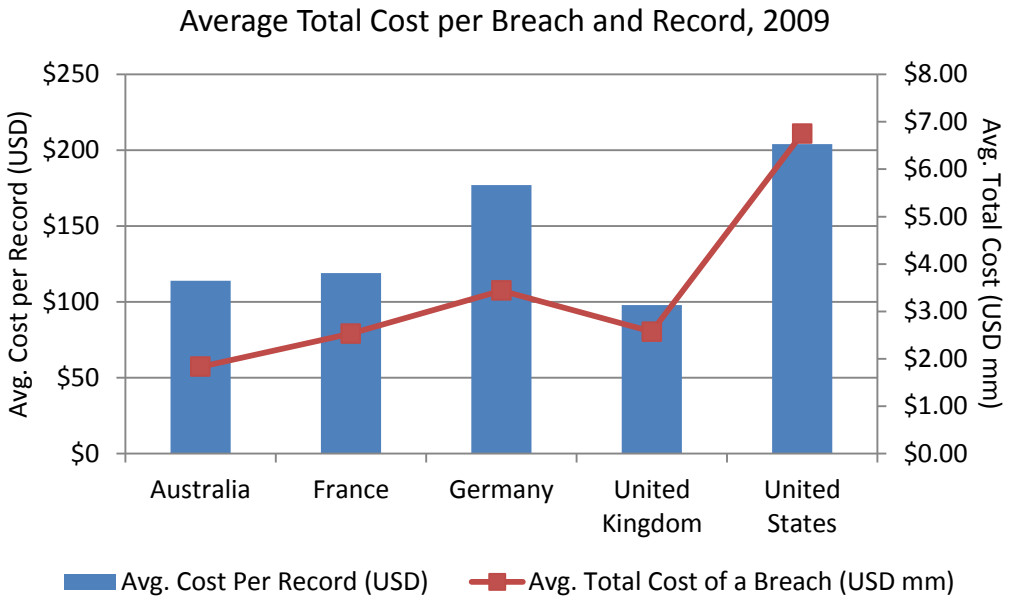
"In April, 2009, the Wall Street Journal reported that ***China was suspected of being behind a major theft of data from Lockheed Martin's F-35 fighter program****, the most advanced airplane ever designed. Multiple infiltrations of the F-35 program apparently went on for years."*

Source: WSJ, April 2009

Country	Avg. Churn Rate: % Customers Lost After Breach	Minimum Total Cost (USD)	Maximum Total Cost (USD)	Minimum Breach Size	Maximum Breach Size
US	3.60%	749,654	30,851,628	5,010	101,000
UK	3.90%	556,933	5,982,083	5,210	60,000
FR	4.50%	341,736	8,564,933	2,520	57,700
DE	4.20%	542,093	8,476,477	3,300	63,100
AU	3.40%	380,296	3,755,417	3,368	65,000

Source: PGP Corporation, 2009 Annual Study: Global Cost of a Data Breach, April 2010

[4] PGP Corporation, *2009 Annual Study: Global Cost of a Data Breach*, April 2010



Source: PGP Corporation, 2009 Annual Study: Global Cost of a Data Breach, April 2010

McAfee®

"Businesses lose more than $1 trillion in Intellectual property due to data theft and cybercrime."

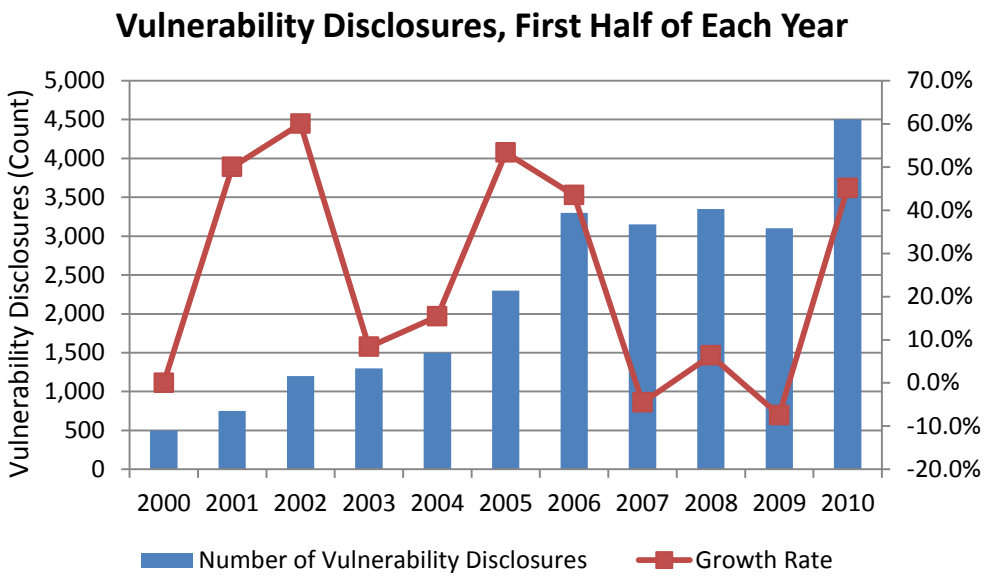
Source: McAFee, 2009

Based on a 2009 study performed by researchers from Purdue University's Center for Education and Research in Information Assurance and Security (CERIAS), McAfee estimates that companies worldwide lost more than $1 trillion in 2009 from cyber attacks. [5] The report, *Unsecured Economies: Protecting Vital Information,* examined responses from more than 800 CIOs in the United States, the United Kingdom, Germany, Japan, China, India, Brazil, and Dubai. The companies surveyed estimated their combined value of lost intellectual property to be $4.6 billion over the last year alone, and spent approximately $600 million repairing damages from the data breaches.[6]

High-profile attacks like GhostNet (2008), Aurora (2009-2010), and Zeus (multi-year) have garnered immediate attention from all sectors of the government and commercial enterprises. One malware program, called Conficker controls over 6.4 million computer systems in 230 countries making it the largest cloud-computing infrastructure in the world - larger than Google and Amazon.[7] Microsoft offered a reward of $250,000 to anyone providing information that led to the arrest and conviction of the creators of the Conficker malware.[8] Even Google, one of the world's most technologically sophisticated organizations, fell victim to a recent Chinese government-sponsored cyber attack, which ultimately served as a wake-up call to the vulnerability of today's network infrastructure.[9]

[5] McAfee, January 2009
[6] The Center for Education and Research in Information Assurance and Security, *Unsecured Economies: Protecting Vital Information,* January 2009
[7] Read Write Web, April 2010
[8] PandaLabs, Annual Report 2009, January 2010
[9] Official Google Blog, January 2010

The pace of these threats is accelerating in 2010, highlighting the urgency that organizations face in finding a solution to this critical issue.



Source: IBM X-Force, Mid-Year Trend and Risk Report, August 2010

Accelerating Cyber Threat

The market for attack software has experienced a recent surge. Strong demand has created a market for online crime that now exceeds revenues generated by the global drug trade.[10] Due to the increased activity in the malware black market, exploits and rootkits, software surreptitiously installed to allow privileged access to a computer without detection, have emerged as an underground commodity routinely traded for tens of thousands of dollars.[7] Organized funded threats are leveraging free market principles to develop illegal cyber weapons that target specific sites, people, and information across all sectors.

MessageLabs

"Online crime is bigger than the global drug trade."

Source: Message Labs, The Online Shadow Economy: A billion Dollar Market for Malware Authors, 2007

In addition to the obvious monetary incentives powering these cyber invasions, there are also well organized, government-sponsored programs initiating attacks in an effort to gain competitive advantages over foreign states. These assaults strive to penetrate foreign corporate and government networks to control the stolen IP and to fortify their own national infrastructure. Russia and China are both well-known for developing some of the most sophisticated malicious code in the world, characterized by the ability to easily bypass leading anti-virus and intrusion detection systems (IDS).

[10] Message Labs, *The Online Shadow Economy: A billion Dollar Market for Malware Authors*, 2007

Countries Developing Advanced Offensive Cyber Capabilities

Because of the vast resources behind these efforts, the attackers are much more advanced than their defensive counterparts.

The Evolved Method of Attacks

Attackers use malicious backdoors, trojans, botnets, and stealth rootkits collectively known as malware, to gain unlimited access to myriad networks. More specifically, it is now common for hackers to develop malware toolkits with the ability to evade detection at the perimeter, effectively trivializing traditional perimeter security software, including anti-virus and intrusion detection systems. These criminals constantly test their malware against the most up-to-date anti-virus solutions in order to remain elusive. The new breed of malware provides an astonishing threat due to its sophisticated architecture, exploiting previously unknown vulnerabilities with custom-written malware, which has proven conclusively and repeatedly to evade detection.

*"**The Commerce Department's Bureau of Industry and Security had to throw away all of its computers in October 2006**, paralyzing the bureau for more than a month due to targeted attacks originating from China. BIS is where export licenses for technology items to countries like China are issued."*

Source: InformationWeek, October 2006

In addition to developing more sophisticated malware, hackers are creating new methods to ensure successful attacks on targeted organizations. As IBM stated in the IBM X-Force 2010 Mid- Year Trend and Risk Report:

> ***"Rather than focusing on a single point of entry, these latest threats aggressively target multiple resources within an enterprise to ensure successful exploitation. No longer are single, public-facing resources the greatest risk, but instead, every employee and endpoint has become a potential point of entry. Sophisticated combinations of vulnerability exploitation, spam, phishing, malicious URLs and social engineering are all easier to obfuscate, automate, and deploy than ever before."***[11]

Although sensitive data is not found on every end node, hackers can utilize infected endpoints to reach other endpoints that have access to critical data or leverage the infected end points to invade other computers. This evolved strategy presents entirely new challenges for any organization with sensitive digital information.

*Both the campaigns of then Senators **Barack Obama** and **John McCain were completely invaded** by cyber spies in August 2008. The Secret Service forced all campaign senior staff to replace their Blackberries and laptops. The hackers were looking for policy data as a way to predict the positions of the future winner. Senior campaign staffers have acknowledged that the Chinese government contacted one campaign and referred to information that could only have been gained from the theft.*

Source: Newsweek, April 2010

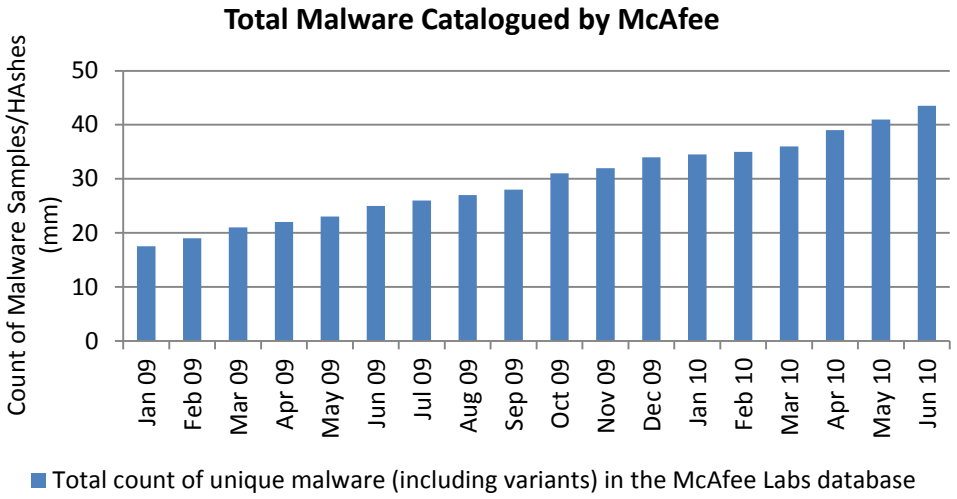
[11] *IBM X-Force, Mid-Year Trend and Risk Report, August 2010*

The Need for Innovative Technology

Due to these ongoing and sophisticated cyber threats, organizations must redirect their security investments to products and services that are much more effective than the commonly used products from the past. First, enterprises need to reevaluate their approach to endpoint protection, which has become the most important issue in an increasingly Web-based, de-perimeterized computing environment.[12] Organizations must also seek scalable solutions that address forensics, which identify the source and extent of the crime, its impact on their business, and the volume of sophisticated malware engaging their network.

Existing IT security investments such as endpoint anti-malware, intrusion detection and firewalls are necessary, but insufficient to detect and block modern threats while protecting enterprise data.[9] These solutions fail because they do not have prior knowledge of the threat, do not understand the malicious behavior of malware, cannot scale with the sophistication and volume of modern malware, and do not secure the end node thereby exposing digital assets to an infinite number of threats.

The graph below indicates the total volume of malware detected by McAfee on a per month basis. As of June 2010, McAfee has catalogued a total of over 40 million different types of malware. Most notably, McAfee has cataloged *10 million* new pieces of malware in the first half of 2010, making this period the most active half-year ever for total malware productions. During the same period in 2009, McAfee discovered 9 million new pieces of malware. Additionally, during 2009, PandaLabs, the anti-malware lab of Panda Security, identified 25 million new malware samples.[13] Prior to 2009, the Company had identified a total of 15 million pieces of malware in 19 years.



The increasing demand for superior security software is inevitable. Entities across all sectors are now unprecedentedly dependent upon Web-based and network infrastructures to store safely their most valuable assets. With the landscape of attack software accelerating in both volume and technological sophistication, organizations will not only demand, but will also be forced to adopt the most advanced defense software in order to thrive in a digitally-based environment.

[12] The 451 Group Research, March 2010
[13] PandaLabs Annual Report, December 2009

Technology and Product Overview

Traditional approaches to Enterprise security are not working. As proven by the recent Google data breach, it is now understood that cyber criminals will succeed in infiltrating even the most secure computer networks. Industry analysts agree that over 80% of the newly emerging malware goes undetected.[14] Overall, corporate and government organizations have lost faith in the ability of anti-virus solutions to protect the end-node because of the success and severity of recent cyber attacks.

Enterprises now demand the ability to detect cyber attacks early, before any critical damage has occurred. Organizations need faster, more accurate and in-depth information detailing the characteristics of advanced cyber threats. When compromises do occur, organizations need to assess the damage and determine whether lateral exploitation has occurred. When attackers have interacted with hosts in the network, the enterprise must completely understand the ramifications of the threat. In order to prevent data breaches sustainably, entities must fully understand the malware's origin and characteristics through key forensics left behind by the malware author.

Google™

"Like many other well-known organizations, we face cyber attacks of varying degrees on a regular basis. In mid-December (2010), we detected a highly sophisticated and targeted attack on our corporate infrastructure ***originating from China that resulted in the theft of intellectual property from Google****."*

Source: The Official Google Blog, January 2010

EXXON Mobil ConocoPhillips MARATHON

The companies – ***Marathon Oil, ExxonMobil, and ConocoPhillips*** *– didn't realize the full extent of the attacks, which occurred in 2008, until the FBI alerted them that year and in early 2009.*

Based on the kind of information that was being stolen, ***federal officials said a key target appeared to be bid data potentially valuable to "state-owned energy companies," providing critical details about new energy discoveries.***

Source: The Christian Science Monitor, January 2010

HBGary's ground breaking product suite addresses these issues by offering a next-generation enterprise threat detection software solution that immediately detects advanced malware and exploitation tools. The Company's products detect sophisticated attack software without the use of signatures and without prior knowledge of the threat. HBGary's products address a number of top security concerns for government, financial, and corporate enterprises, including cyber-espionage, identity theft, insider threats, and the theft of proprietary information.

[14] ZDNet, July 2006

End Node Security vs. Perimeter Security

One of HBGary's key differentiating features is their unmatched ability to secure the end node. There are several advantages to end node security solutions over traditional perimeter solutions.

First, if malware is packed or encrypted, perimeter security devices cannot access the packets' interior, rendering these solutions useless in diagnosing malware. The perimeter solution must decrypt the encryption code in order for the security product to diagnose the potential malware. Most existing perimeter products currently do not posses this ability and, thus, fail to provide an adequate defense solution.

Gartner

"For several years, the most damaging attacks have used targeted custom malware that evades traditional anti-virus and Web security gateway controls. ***HBGary provides a set of products for analyzing executables and system configurations to detect, inspect and analyze advanced malware, based on its patent-pending Digital DNA technology."***

Source: Gartner Research, April 2010

Second, much malware executes during download, meaning an individual must first open a link, download a PDF, or insert a flash drive in order for the malware to be initiated. This attack proves very successful against computer networks reliant upon perimeter security because the malware is presented to the user in the form of a standard email or recognizable file format, which is very difficult for perimeter security solutions to detect.

Third, perimeter security is ineffective against attacks on individual users – phishing attacks – because existing perimeter security cannot account for poor user judgment and irresponsible computer activity, such as clicking on infected links.

the 451 group

"At a baseline, ***HBGary specializes in forensic tools that help analysts understand the behavior of malware, post-infection, in minute detail.*** *But the company has begun aggregating its forensic intelligence into more genotypic malware definitions that can be used to detect sophisticated, zero-day threats in the absence of a signature, and to categorize and rate those threats by severity."*

Source: The 451 Group, March 2010

In addition, perimeter software is not scalable due to the sheer volume of data that continually and freely flows across the perimeter. Traditional perimeter solutions are not equipped to monitor this amount of data. It is extremely resource exhaustive, and in many cases mathematically impossible, to decrypt and disassemble each and every packet that engages the perimeter. As a result, inspection at the perimeter is shallow, ineffective, and drastically reduces performance.

To increase efficiency at the perimeter, signatures are deployed to look for "*known*" malware. If "unknown" packets are inspected, the information is delayed when reaching the end node creating significant performance issues. Given the resources required to scan all unknown potential malware as well as the volume of potential malware that passes through the end node, perimeter security simply does not scale enough to diagnose and analyze every source of potential malware. Therefore, it is literally impossible for these solutions to prevent a significant amount of malware from penetrating the network.

HBGary's threat detection solution is unique in that it does not rely on perimeter protection and all the inherent flaws in that model. Instead, the Company monitors all applications and processes running in memory, at the end node, in order to detect malicious code. In memory malware must decrypt itself to pose any threat, therefore, the Company's technology naturally defeats packing and encryption because the data is already decrypted by the time HBGary analyzes it.

Unlike HBGary, perimeter security solutions must actively decrypt malware at the perimeter because malware is always encrypted when it reaches the perimeter. Once the encrypted malware evades the perimeter security, it can then decrypt itself in memory, penetrate the system and finally infect the greater network, all while avoiding detection by the perimeter security system. Since all applications and malware must run in memory (RAM), HBGary detects the vast majority of malware in the network by focusing their efforts on securing the end node.

Besides simply protecting malware that flows through the perimeter, by focusing on the end node the Company is uniquely suited to address the risks of social networking attacks, phishing attacks, booby-trapped documents, and drive-by downloads resulting from irresponsible internet usage by end users.

Technology

HBGary's incomparable product suite is powered by sophisticated, game-changing technology that is unique among all other solutions available in today's market.

The powerful technology serves to uncover evasive malware, previously undetectable, by running in memory rather than executing as a permanent application on the infected host's file system. In order to accomplish this feat, HBGary devoted years to researching the data structures of Microsoft's Windows operating system, including the way in which the operating system allocates and manages memory. Leveraging this knowledge, HBGary has the ability to reconstruct captured Windows images, including virtual memory, with complete accuracy. The Company can then analyze program execution at a granular level – memory allocation, library and processor access, registry writes and edits, etc. – to fingerprint malware executables, view changes linked to malware infection or other activity and extract forensic information from memory post-infection.

From a bottoms-up approach, the base layer of HBGary's core technology holds the physical memory analysis. Layered over the base layer is a disassembly and dataflow engine that can examine and take apart any software. This allows HBGary to recover all software behavior for every running code object in physical memory meaning, HBGary can recover all software running on a system at the time of analysis.

According to Deputy Secretary of Defense William Lynn, ***the most significant compromise of military computers known to date began after an infected flash drive was inserted into a US military laptop at a base in the Middle East.*** *The malicious code on the drive spread undetected on both classified and unclassified systems establishing what Lynn describes as a digital beachhead that allowed the attackers to transfer data to servers under foreign control.*

Source: Voice of America News, August 2010

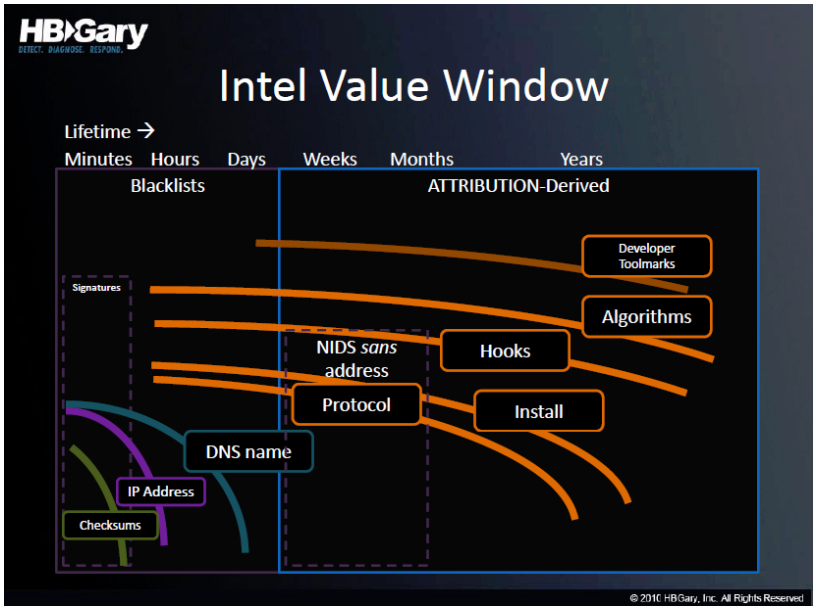
The next layer applies rule-matching over the recovered behaviors to identify the malwares' threat level. The rule-matching capability is HBGary's patented pending Digital DNA technology, the basis for all HBGary technology. Finally, Responder and Active Defense are layered on top of Digital DNA. **HBGary's technology represents a very high barrier to entry that is difficult, if not impossible, for competition to replicate**.

Extracting critical evidence from the end node, which is exponentially more effective than perimeter solutions, HBGary's technological sophistication is found in their ability to detect security threats in the physical memory and to dive deep into the code base to examine and disassemble every line of malicious code. Once malware is detected, HBGary's technology breaks down, analyzes, and classifies the traits of the malicious code to prioritize all active malware in the system by actually scoring the malware based on the severity or threat level of the malicious software. The malware is prioritized based on HBGary's analysis correlation engine scoring algorithm. Next, the Company stores and records the new malware while also crosschecking it against their robust and ever-growing proprietary database of malicious code. This correlation & classification system can be easily extended to locate nearly any type of data. In addition, maintenance of this system is easy.

Once the new malware is compared to those in HBGary's database, the Company can match all relative malware to the development source based on the code's unique traits. This information can then be presented in a clean, interactive, easy to understand scatter plot or link analysis environment. The graphic analysis details and tracks the various code traits to the developer of the malware. Note that most malware developers reuse core code for new types of attacks, and this information is used to link different attacks back to its original source. With HBGary's unparalleled technology, the average IT member can quickly and accurately identify the most severe malware on any system, and also determine the number of unique sources currently attacking the system within a matter of minutes.

A similar result with the competitions' most sophisticated solutions would require a skilled and experienced reverse engineer to work for a week. With HBGary's technology, this process takes 10 minutes performed by an average IT person. The Company separates itself from the competition through its advanced software, which yields effective and accurate threat detection solutions requiring minimal IT support or reverse engineering.

Hackers rarely alter the specific algorithms and developer toolmarks over the course of the malware's lifetime; as opposed to checksums or IP addresses which can be altered on a per minute basis. Thus, the code base and developer toolmarks are not only the best indicators to examine, assess, and classify potential malware but also to archive for future reference and scanning.



Digital DNA™

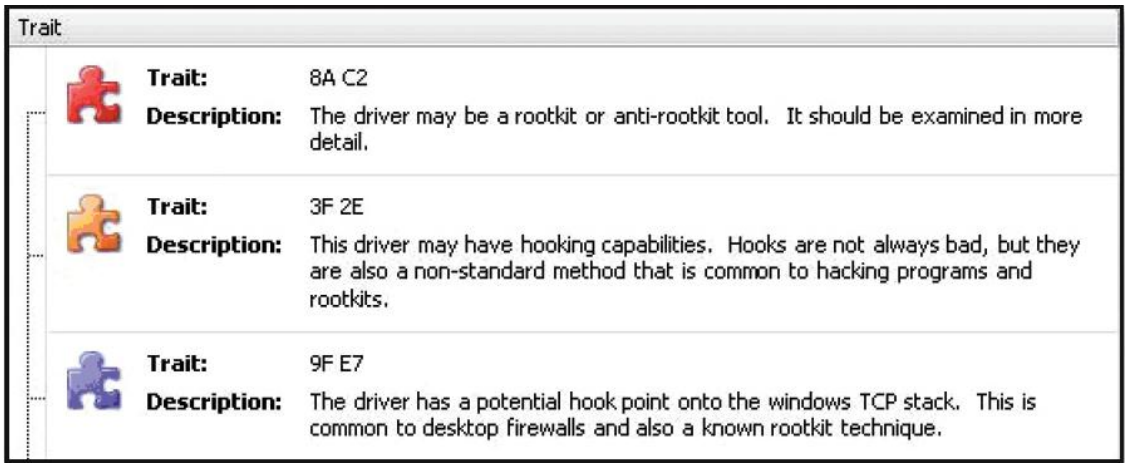
Digital DNA™**,** HBGary's patent-pending core technology, is the basis for all HBGary products, both enterprise and stand-alone. Digital DNA is the first live memory and runtime analysis platform to detect today's most advanced malware by examining the software's behavior, rather than relying upon checksums or signatures. HBGary's technology enables customers to analyze memory quickly, easily and to see all running programs executing on the relevant machine. Advanced detection technology is able to identify stealth techniques used by cyber criminals and state sponsored threats. Once suspicious behaviors are found, the suspect binaries can be easily disassembled and debugged to identify their true intent and capabilities.

"I tested Digital DNA in a challenge and found that if this had been a real breach, I would have been able to initiate action within 3-5 minutes. This would be a real cost saving, which is important in a corporate environment."

- Chief Advisor, Enterprise Risk and Security, Large Telecommunications Firm

This patent-pending technology detects advanced computer security threats within physical memory without relying on the Windows operating system. In the event of a data breach, the operating system cannot be trusted due to possible contamination. **The reliance on the operating system to query information is a key weakness in traditional host-based security products.** HBGary's advanced detection technology does not use the OS and is able to identify techniques used by cyber criminals and state sponsored threats. Most importantly, all software modules residing in memory are identified and ranked by level of severity through the 'Digital DNA Sequence'. HBGary's 'Digital DNA Sequence' appears as a series of 'trait' codes and when concatenated together describes the behaviors of each software module (more information on Digital DNA Sequence below).

Malware threats are automatically detected on endpoint nodes and displayed on the dashboard console with behavioral traits that provide metadata threat intelligence.



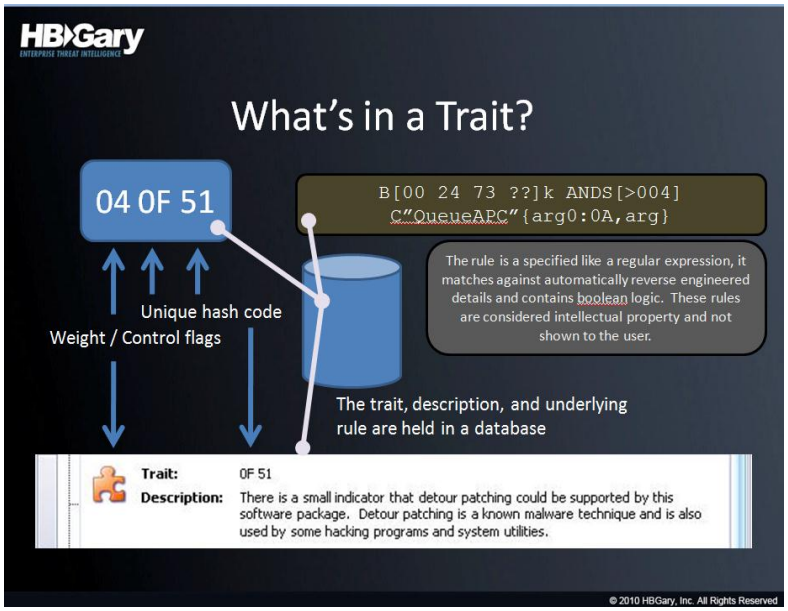
Once the malware and suspicious binaries are detected, Digital DNA compiles a weighted sum of program behaviors to determine if the program is suspicious. This creates the Digital DNA sequence for the binary. If the weighted sum is over a certain value (30.0) the program is considered suspicious.

The graphics below shows color-coded alerts of compromised computers, suspicious software modules, threat severity scores, and behavioral traits. Users quickly identify infected computers, the discovered malware, and descriptive metadata about the malware.

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	intelppm.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

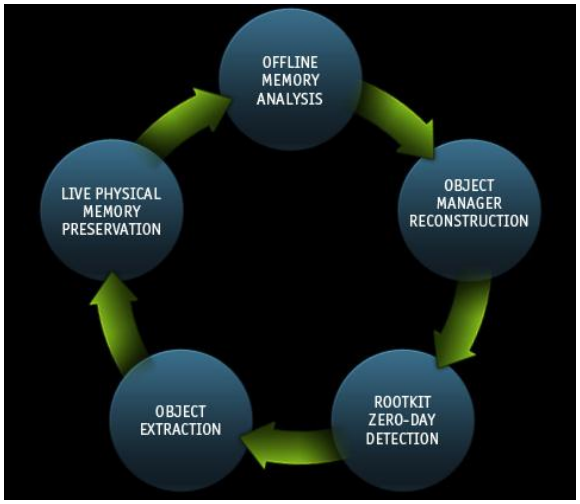
Detected malware can be contained by searching the network for its variants. The malware is then extracted from the memory of remote computers for further analysis and attribution. **The enterprise-wide capability to search physical memory is unique to HBGary - no other vendor has a technology that can compare.**

Digital DNA is implemented under-the-hood as a custom language that resembles regular expressions. HBGary has developed a lexer and grammar for this language, which is integrated directly into the engine that processes physical memory and software disassembly. Each numerical triplet corresponds to an individual rule that has been expressed in the detected software object. Each of these expressed rules are called 'traits'.



The sequence of all traits for a given software object is called the 'Digital DNA Sequence' for the object. Each individual trait is backed by both a human-readable description and a rule that resembles a regular expression. Digital DNA is a powerful concept. It can be used to enumerate the properties of any digital object. Generally speaking, it can be used to rank and classify any digital object into a set. This technology is patent pending.

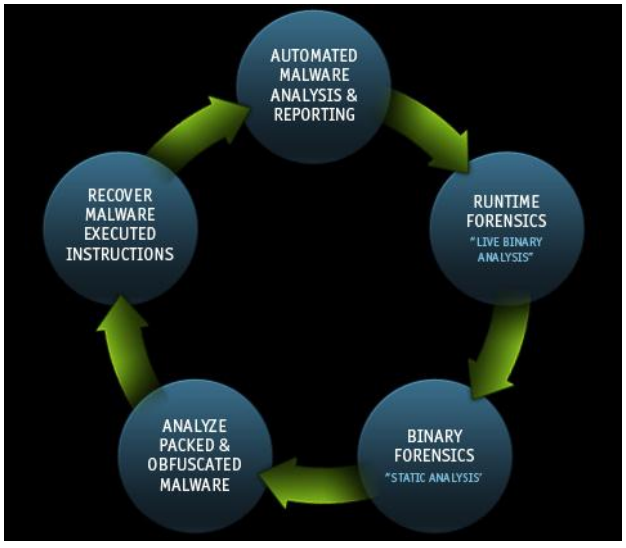
Live Memory Acquisition and Diagnosis Process
This diagram illustrates the process by which HBGary culls and extracts memory during the diagnosis process. The memory acquisition is performed using a special signed driver and is available as a stand-alone tool as well as integrated with HBGary's enterprise product. Many law enforcement organizations standardize on HBGary for memory forensics, including the FBI and the Secret Service.



Forensics: Robust Malware Database
Backing up the technology is HBGary's Threat Monitoring Center. The Company processes over 17,000 malware samples per day, while also categorizing the malware and constantly testing their current products against the newly catalogued malware to ensure detection. Forensic tool marks unique to malware authors are culled and put into the products, thereby allowing HBGary to track individual developers. HBGary calls this information the "global threat genome", which customers can query to reference and crosscheck other malware traits.

From a forensics perspective, critical information in memory is essential for winning court cases and documenting suspect activities. Almost all data can be recovered in memory including social media technologies, keys, passwords, complete internet histories, among others. With HBGary, machine memory is easily preserved and analyzed, by providing a complete "snap shot in time" of the running systems.

In addition, HBGary has the ability to read VMWare memory snapshot files from both the VMWare workstation product and also the ESX server product. This means that HBGary can be used alongside cloud services to detect malware within instanced virtual machines. This capability can easily be extended to other VM solutions. This is significant because as virtual machine technology becomes more prevalent, attackers will look to find ways ways to store their malware in the cloud.



The diagram to the left displays the binary and runtime analysis used to disassemble and analyze the malware code base. This entire process can be run outside of the virtual host and integrated directly into a VM platform.

Responder™ Platform: Automated Memory Analytics

The HBGary Responder platform is designed to perform a comprehensive live Windows memory investigation. Responder allows analysts and investigators to preserve the entire contents of live memory and page file on the Windows operating systems in a forensically sound manner. Responder then analyzes and diagnoses the memory image to reveal the operating system, user, and application information critical to computer investigations.

"Responder exceeded expectations. Responder™ is a need to have product, not a nice to have."

- US Department of Commerce

Harvested information includes both kernel and user-mode objects, structures, binaries, and other useful artifacts. When malicious or suspect applications, drivers, and other executables are found, Responder can seamlessly extract the file(s) from the memory image retaining portable executable (PE) structure so they can be further diagnosed, executed, and monitored in their unpacked state.

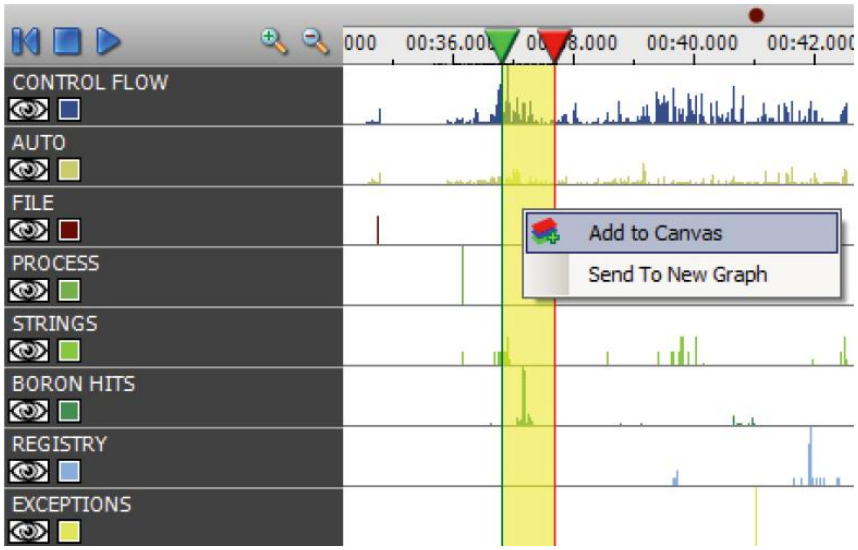
the 451 group

"As Hoglund points out, there are hundreds of thousands of different keylogger programs, but only a handful of ways to sniff keystrokes on a Windows system. HBGary focuses on the latter, rather than the former, in identifying threats. That kind of capability, in addition to ***HBGary's deep pool of experts and knowledge base of threats, is an increasingly valuable commodity for diversified vendors that want to boost their professional services capabilities (McAfee?) and also increase their understanding of advanced malware and the cybercrime underground****."*

Source: The 451 Group, March 2010

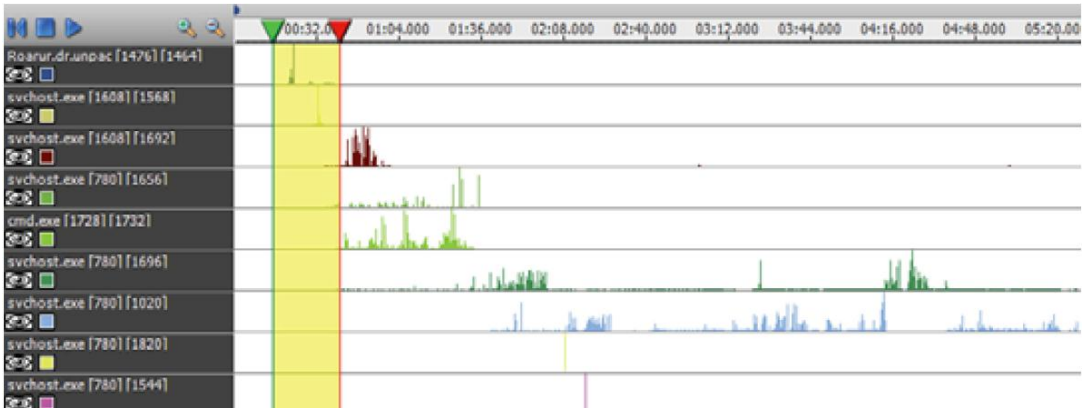
Because Responder draws information from raw physical memory, the methodology allows Responder to defeat many packers and other obfuscation techniques used by malware writers. In particular, the software behaviors used by Digital DNA are not masked, and actionable intelligence such as IP addresses and URL paths are exposed. Following binary extraction, analysts can apply Responder platform's reverse engineering tool to perform static and runtime disassembly rapidly identifying stealth activity, file system changes, registry modifications, network activity, encryption/decryption routines and other malicious code characteristics. This is one reason why HBGary's technological capabilities far surpass traditional anti-virus solutions.

REcon™



REcon is a leading-edge technology that records and graphs malware behavior at runtime so organizations can extract critical data from unknown executables. REcon represents the most complete tool to recover actionable intelligence from malware, including how the malware installs, survives reboot, and communicates to the Internet. In addition, Recon also tracks the contents of decrypted buffers and the bypassing of executable packing. **REcon records execution at a single step resolution, while also sampling data, and does this at such high performance that, while tracing a GUI based application, the traced application's GUI can still be interacted with. This is a revolutionary feature that no other debugger can match.**

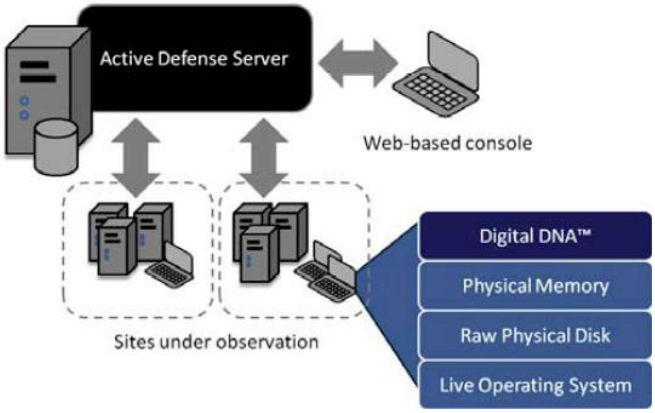
When used to trace malware, this powerful technology provides incident response teams with a single tool that is forensically sound and easy to use. Recon allows small security teams to automate analysis giving them run-time information, such as decrypted copies of otherwise encrypted network traffic, registry key activity, filesystem activity, and advanced behaviors such as process-injection. For larger teams, it allows a deeper analysis, without the overhead of manual reverse engineering, as well as assistance incorrelating pertinent streams of information.



Analysts requiring a deeper understanding of malware or suspicious applications can use REcon to perform binary and runtime forensic analysis with run trace, data flow tracing, and debugging capabilities. REcon is a very powerful technology that can be integrated into a variety of products. For example, a company that sought to execute suspicious documents in a VM could use REcon and Digital DNA to detect malicious documents. Going beyond a single VM, the REcon technology can be executed in a large farm of VM's, scaling linearly. This could be a critical component added to a SOC/CERT team, and would be a unique product that is highly sought after by the U.S. Government. Finally, if a web front end were placed on REcon, it could easily complete with a product like CW Sandbox.

Active Defense

Leveraging HBGary's patent-pending core technology, Digital DNA, Active Defense is the first next-generation enterprise threat detection software solution capable of immediately discovering advanced, unknown malware and exploitation tools without signatures or prior knowledge of the threat on disk, or in all physical areas of memory, across the entire enterprise at once.



Active Defense is HBGary's enterprise version of Digital DNA combined with an extensive suite of live forensics and response capabilities. Active Defense includes all the features customers expect from Digital DNA, as well as concurrent enterprise scanning and forensic analysis for disk, live operating system, memory, and behavioral based threat detection through ongoing RAM snapshots. Not only is Active Defense the fastest solution on the market for detecting advanced threats (i.e., forensically sound NTFS disk scanning at 4 GB per minute concurrently), but also the Company's enterprise console is easy to use. **In fact, running queries across the enterprise with Active Defense is no more complicated than using Google's 'advanced search' feature.**

Powered by its state-of-the-art analysis correlation engine, which ranks various malware currently in the system based on threat level, Active Defense provides the average IT member with the ability to distinguish, compare, and identify malicious code. Traditionally this has been beyond the capability of IT staff, and all suspicious programs were sent to the AV vendor. With Active Defense, an IT staffer skilled enough to read a packet sniffer can now respond to malware. **This enables incident response for organizations that have overtaxed IR teams, or that have not traditionally been able to justify having an internal IR practice.**

All software modules residing in memory are identified and evaluated by level of severity. The Digital DNA sequence appears as a series of trait codes, which when connected, describes the behaviors of each software module. Digital DNA is used because it is easily understood by non reverse-engineers. There are only a handful of similar products in the space, all of which are complicated to use and must be operated by an incident response professional who is an expert at reverse engineering or incident response to achieve similar results. More importantly, HBGary's Active Defense is the only product in

the space that offers enterprise wide physical memory assessment and detection of unknown threats via Digital DNA.

Active Defense has the ability to scan thousands of end-nodes concurrently and provide critical threat intelligence necessary for government and other organizations to determine a course of action. Other Active Defense capabilities include the following:

- Variant traits found by scanning using Digital DNA
- Quick access to file, DLL, and exe, created around the time of the attack
- Forensically sound snapshots and disk analysis
- "Actionable intelligence" allowing existing solutions to block the attacks (i.e., NIDS)
- Custom inoculation shots so customers no longer depend on a .dat update from an anti-virus vendor and can clean a host without incurring the cost of re-imaging.
- Permanent inoculation so the host is now immune to that particular attack vector
- Creation and scanning for indicators of compromise (IOC) to identify compromise, advanced persistent threat, lateral movement, malware variants, and to rapidly identify the scope of an infection, allowing non-infected machines to stay on line
- Identifying the type of exploit tools used in the attack and the initial point of infection
- Information tracing the attackers lateral movement within the network (command line usage, pass-the-hash, downloaded tools, etc)
- Identifying compromised credentials and previously compromised data
- Extracting timeline information from hosts, critical to reconstructing events

FastDump – A Memory Acquisition Tool

Fastdump is the industry's most forensically sound Windows memory dumping utility. Its memory footprint is smaller than any other offerings currently in the market. All required code is statically linked, which eliminates the need for additional dynamic-link libraries (DLLs) to be loaded, yielding an executable size of only 80K.

Like all HBGary products, Fastdump is easy to use. It requires only a USB stick or similar means to initiate a command prompt on the target Windows system. The user then simply types "fd.exe," where the filename is the dump file, and Fastdump will take a snapshot of the physical memory. This file will be a binary dump of RAM. The size of the resulting file will depend on the amount of RAM present in the target machine. Since Fastdump is optimized to work with USB transfers, it will perform well even when dumping to a USB drive.

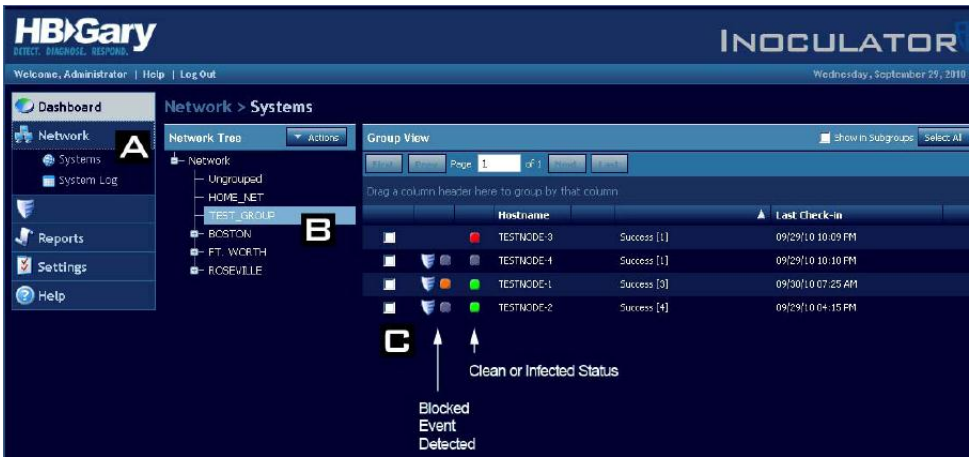
rockyou

*"In December 2009, a **major password breach occurred that led to the release of 32 million passwords.** Further, the hacker posted to the Internet the full list of the 32 million passwords (with no other identifiable information). Passwords were stored in cleartext in the database and were extracted through a SQL Injection vulnerability."*

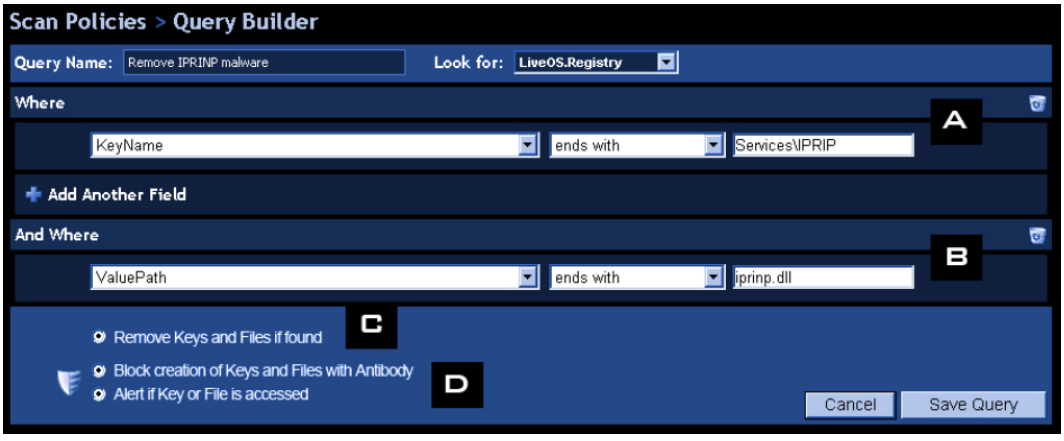
Source: Imperva, 2010

Inoculator – Available Q4, 2010

The Inoculator is designed to detect, remove, and prevent further infection of known malware. It puts the power of remediation in the hands of the customer, allowing customers to remediate without having to wait for their antivirus vendor. What makes this product so revolutionary is that the inoculator does not use agents. Instead it manages all end-nodes using standard windows-networking API's over the network. Inoculator interfaces with the Active Directory server and communicates with hosts using remote procedure calls only. No agents or executables are placed on any of the end-nodes and machines are managed using a group interface. This provides a tremendous benefit to customers and there is nothing else like it on the market.



The inoculator uses scan policies to detect known malware. A scan policy specifies the files and registry keys that the malware uses to maintain persistence on a system. The user has the ability to specify, in detail, what registry keys and files are used by the malware. If the malware is found, the system will alert the user. If the user has configured the system to clean the malware, it will be removed and the system will remain in a clean state. Finally, if the user chooses they can also block the system from further infections. This forms a sort-of tripwire that will send a live alert if something or someone attempts to infect the protected host.



Capabilities of HBGary's product suite include the following:

- Detects zero day malware or targeted malware, through HBGary's code level analysis of software in physical or virtualized memory
- Acquires and analyzes physical memory (RAM) images at the lowest possible level in a forensically sound manner with full support for Windows 32 and 64 bit platform. HBGary is the only company in this space to have full platform coverage with the ability to collect the pagefile and over four gigabytes of RAM
- Organically scales to monitor hundreds of thousands of end-nodes by monitoring RAM, rather than relying upon perimeter security solutions
- 'Carves' and reconstructs the operating system state from only physical memory, in both real and virtual environments, providing an extremely high barrier to entry for competitors looking to join this space
- Extracts running binary code and modules from physical memory. This feature defeats packing, polymorphism, hidden hooks and obfuscation, all of which defeat traditional anti-virus and intrusion detection systems
- Recovers code and data from binary executable objects
- Disassembles binary executable objects and reconstructs logic pathways. HBGary is the only solution that uses code-logic to determine behavior. All other existing solutions use only binary indicators that are unrelated to code behavior, thereby inaccurately classifying malicious code traits
- Scans memory and reconstructed objects for behaviors and symbols to provide the most accurate understanding of the malware characteristics
- Presents human-readable technical information about binary object behaviors

Managed Services
As experts with years of experience in attack technologies and malicious software design, the HBGary team helps organizations analyze and capture malware for encryption routines, backdoor capabilities, command and control functions, exfiltration and covert channels, as well as bypassing packing and anti-forensics layers. HBGary allows customers to discover the exploits, tools, and resources used to compromise customers' infrastructure.

The managed Active Defense service enables customers to utilize HBGary security professionals in managing the day-to-day triage and analysis of suspicious behaviors relative to the entity. Derived from the Company's deep domain experience in both attack and defense technologies, the following services are provided by HBGary's team:

- Analyze subtle fingerprints of the tools and techniques used to exploit infrastructure
- Reconstruct the attack utilizing trace evidence
- Identify the vulnerable areas of your infrastructure that permitted the intrusion
- Advise customers to help avoid future attacks
- Determine the geographic origin of the attack

HBGary's world class services include:

- Continuous scanning for compromises and new attacks, weekly scan reports, and immediate notification for any found vulnerability
- Detection of unknown threats using Digital DNA and follow-up analysis by an HBGary security engineer. Found malware is fully reverse engineered, including command-and-control so that intrusion detection software (IDS) signatures can be generated. This allows actionable intelligence for immediate response and an auditable report for compliance purposes
- Continuous monitoring for known threats using indicators of compromise (IOC) that are specific to the customers' environment, including threats known to attack that client's particular environment
- Attribution in which threats are evaluated for targeted behavior including human interaction within the system, allowing management to determine the appropriate legal course of action
- Damage Assessment at which point HBGary performs forensically sound remote-assessment of the endpoint to reconstruct a timeline of malicious behavior, detect theft of data, stolen credentials, and whether lateral movement has occurred
- Remediation – Offered only by HBGary, the Company removes infectious malware or remote access tools using the Inoculator whenever possible. HBGary security engineers expertly use the Inoculator to remove malicious code without incurring the cost of reimaging a machine

HBGary Acquisition

Since its inception in 2004, HBGary has developed cutting-edge defense security software to detect the most advanced malware to date. With advanced persistent threats growing exponentially in both count and sophistication, HBGary is poised for explosive growth. Given the scope of the opportunity the Company faces, HBGary would benefit from the additional infrastructure and resources that come from a larger firm, in their efforts to fully capitalize on this exploding market. An acquiring firm can easily leverage their greater platform to immediately gain a significant competitive advantage over their competition. By introducing the Company's products into a wider distribution system and greater installed base, an acquiring entity can realize the financial benefits resulting from the significant market demand for this differentiated technology.

Because HBGary has created such a broad and innovative product offering, they will be able to add significant value to any network security software or services provider. HBGary will:

- Add value to outdated security technologies and increase the lifetime value of existing products and solutions
- Provide a tremendous upsell opportunity
- Offer any security provider a significant competitive advantage in the often commoditized, ultra-competitive sales process
- Give an acquirer the opportunity to extend existing product lines, allowing the company to both further penetrate existing customer as well as target new potential opportunities
- Provide an acquirer with access to HBGary's high profile customers, which include government agencies, fortune 500 companies, government contractors, and global banks
- Deliver tremendous synergies on both the product and revenue sides

Industry Accolades

HBGary has been recognized both by customers as well as industry analysts for delivering cutting edge security solutions that are changing the way large enterprises conceptualize securing their most important and sensitive assets.

Gartner, Cool Vendors in Application Security, 2010:

For several years, the most damaging attacks have used targeted custom malware that evades traditional anti-virus and Web security gateway controls. HBGary provides a set of products for analyzing executables and system configurations to detect, inspect and analyze advanced malware, based on its patent-pending Digital DNA technology. The company's Responder platform offers advanced tools for preserving and analyzing system to memory to detect and investigate compromises. Other products provide software agents to place on critical servers and PCs to limit the impact of malware and preserve runtime forensic information. The combination of these capabilities can provide visibility into target attacks, botnet compromises and other forms of what the U.S. Department of Defense (DoD) now calls "advanced persistent threats."

The 451 Group, E-Crime and Advanced Persistent Threats, March 2010:

By understanding key elements of Microsoft Windows memory management architecture, HBG has developed tools that can reconstruct captured Windows images (including VMs) with total accuracy and then step through program execution at a granular level, showing memory allocation, library and processor access, etc. – and then use that unique information to fingerprint malware executables, changes linked to malware infection or other activity, and extract forensic information from memory post-infection.

At a baseline, HBGary specializes in forensic tools that help analysts understand the behavior of malware, post-infection, in minute detail. But the company has begun aggregating its forensic intelligence into more genotypic malware definitions that can be used to detect sophisticated, zero-day threats in the absence of a signature, and to categorize and rate those threats by severity.

As Hoglund points out, there are hundreds of thousands of different keylogger programs, but only a handful of ways to sniff keystrokes on a Windows system. HBGary focuses on the latter, rather than the former, in identifying threats. That kind of capability, in addition to HBGary's deep pool of experts and knowledge base of threats, is an increasingly valuable commodity for diversified vendors that want to boost their professional services capabilities (McAfee?) and also increase their understanding of advanced malware and the cybercrime underground.

Big Consulting Company:
"Digital DNA is a game changer."

VP eCrime Unit, Fortune 50 Bank:
"Responder with Digital DNA is definitely a need-to-have item in our toolbox. The options available to dissect the memory are excellent and easy to understand, not like some other tools that are currently in the marketplace."

Chief Advisor, Enterprise Risk and Security, Large Telecommunications Firm:
"I tested Digital DNA in a challenge and found that if this had been a real breach, I would have been able to initiate action within 3-5 minutes. This would be a real cost saving, which is important in a corporate environment."

U.S. Department of Energy:
"Responder is the best new software that I have seen in the last 10 years."

Air Force 92nd Squadron:
"We love Responder and Digital DNA."

U.S. Department of Commerce:
"Responder exceeded expectations. Responder is a need to have product, not a nice to have."

Security Manager - Bankcard:
"I could replace people with this tool, not that I would."

Telindus:
"You can tell how much thought HBGary put into this tool. Love it!"

VP eCrime Unit, Fortune 50 US Bank:
"Responder with Digital DNA, it is definitely a need to have item in our tool box. The options available to dissect the memory are excellent and easy to understand, not like some other tools that are currently in the marketplace."

Government Computer News:
"Fingerprinting also could produce immediate results by implementing it in anti-virus and intrusion detection tools. Traditional signatures used to identify known malware can easily be changed, which limits the life of a given signature and the effectiveness of signature based detection. But tool marks in the binary code can go back for years and digital fingerprints from the malware's source code are less likely to change frequently. This could extend the useful life of a signature from days to years."

Key Customers

Many of the largest and highest profile corporations and government agencies trust HBGary to secure their most valuable information. Select HBGary customers include:

Financial:
Citigroup
Bank of the West
Fidelity
Morgan Stanley
JP Morgan
State Street

Government Agencies:
Department of Homeland Security
National Security Agency Blue Team
92nd Airborne
Federal Bureau of Investigation
House of Representatives
Department of Justice
Centers for Disease Control
Transportation Security Administration
Defense Intelligence Agency
Defense Information Systems Agency
US Immigration and Customs Enforcement
US Air Force

Government Contractors:
Boeing
General Dynamics
Merlin International
Northrop Grumman
SAIC
Booz Allen Hamilton
United Technologies

Fortune 500 Corporations:
Coca-Cola
Sony
IBM
General Electric
Cox Cable
eBay
Best Buy
Pfizer
Baker Hughes

Case Studies

Large Financial Organization
March 2009 - A zero-day spear phishing attack bypassed the bank's layers of security defenses. The malicious PDF document looked legitimate and was opened by an executive. Processes were injected into Internet Explorer and Svchost.exe to use the Internet connection and download the "real malware". Five different applications were downloaded and installed in "stages" to build the modular malware that would remain installed. This malware installation technique is used to bypass scanning engines and is designed to fly under the radar. Digital DNA identified the original PDF as a threat. Digital DNA was used to identify all compromised machines in the network prior to anti-virus having a signature.

Large Entertainment Company
One of the largest entertainment companies in southern California currently uses Digital DNA to verify whether viruses are properly cleaned by an anti-virus signature file. Statistics showed that 50% of all machines were still compromised after being cleaned by the anti-virus signature file. The Company suspected an employee of stealing "Priority Two" information off PCI servers in Los Angeles from their manufacturing plant in Tijuana. They imaged the suspect's computer using HBGary FastDump Pro. Included in the memory image was the password to a Google account, not authorized by the company. Forensic examiners from the company logged into the Google account and found credit cards taken off corporate PCI servers from customers who downloaded music. Total investigation took 8 hours from start to finish including arresting employee. Prosecution of employee is moving forward.

Large Pharmaceutical Company
During the Conficker.C outbreak, the organization thought the malware was contained after they discovered 100 machines infected with anti-virus software. A new scan with Digital DNA revealed there were 113 more machines infected with variations of malware that the anti-virus software did not detect. Digital DNA discovered six new versions on 113 machines. The organization was able to send malware samples and intelligence to their anti-virus vendor for signatures. The security team was able to discover all infections using HBGary Responder Pro to identify the source of the infections.

Consulting Company
The Company's intrusion detection system (IDS) triggered an alarm related to the Blaster worm. It turned out that the two hosts involved were a server that gathered backup images from VMware ESX servers and sent the images to the backup server. From the IDS signature, it appeared that the source host was attempting to communicate on SMB port 445, and appeared to be sending a TFTP command to retrieve a system file. The payload also indicated that this activity was the result of a Blaster exploit being launched.

One theory explored the notion that VMware images being backed up could be infected with the Blaster worm. The next logical step would be to get a current dump of memory from the server and also a copy of memory from the restored backup. "I used HBGary to dump the memory along with the page file. I then imported it into Responder product. HBGary was able to map the part of memory with the suspicious keywords back to the mcshield.exe process. The keywords were part of virus definitions for McAfee that had gotten written to the page file. McAfee decodes these definitions in memory which is why they were not found on the disk with a strings search. I also found several other malware related keywords in these same processes for other definitions. With this information, I was able to white list this activity between the VMware ESX server and the backup server."

U.S. Government Agency & U.S. Department of Defense

One agency was using a freeware memory tool and found a piece of malware on a computer. Analyzing the memory image, they found two Websites that "could have" contributed to the malware infection and these sites were blocked. Analyzing the same image using HBGary Responder Pro, the agency was able to find a total of 6 Websites where malware was downloaded as well as information about ports used and was able to fully analyze malware and determine whether additional machines were infected. Memory Forensics and HBGary Digital DNA are used by some of the most advanced computer network defense teams in the US Government today for computer intrusions, incident response, and enterprise malware detection. These teams employ standards and best practices for detecting advanced threats, diagnosing the nature of the threat so that they can rapidly obtain root cause analysis and improve enterprise policy fast to mitigate the threat.

Management Team

Greg Hoglund
Chief Executive Officer
Greg Hoglund has been a pioneer in the area of software security. After writing one of the first network vulnerability scanners (installed in over half of all Fortune 500 companies), he created and documented the first Windows NT-based rootkit, while founding www.rootkit.com (rootkit.com) in the process. Greg went on to co-found Cenzic, Inc. (cenzic.com) through which he orchestrated numerous innovations in the area of software fault injection. He holds two patents. Greg is a frequent speaker at Black Hat, RSA and other security conferences. He is co-author of Exploiting Online Games (Addison Wesley 2007) and Rootkits: Subverting the Windows Kernel (Addison Wesley 2005) and Exploiting Software: How to Break Code (Addison Wesley 2004).

Rich Cummings
Chief Technology Officer
Rich Cummings has been focused on catching cybercriminals for over 10 years. Rich has been doing incident response investigations since the late 90's when he worked as part of the 911 emergency response team at Network Associates. During his career, Rich has been involved in many high profile incident response investigations at some of the largest companies in the world. Prior to joining HBGary, Mr. Cummings was with Guidance Software for 6 years as the Director of Security Engineering and Government Solutions. Rich was instrumental at Guidance in the early days crafting the enterprise go to market strategy for their flagship product Encase Enterprise. During his time at Guidance Rich held many leadership roles in the organization in product engineering, sales, and marketing departments. Rich also worked closely with the federal government and military to architect large scale solutions for incident response, computer network defense, and counterintelligence investigations.

Penny Leavy
President
Penny Leavy co-founded Cenzic (formerly known as ClickToSecure, Inc.) with Greg Hoglund. She formulated Cenzic's basic business structure, assembled a solid executive team and helped secure financing from top-tier venture capital firms during a tight economy. Previously, she was head of sales for FTP Software building a distribution network of over 500 OEM and channel partners, and open nine international sales offices, growing sales from $3 million to $120 million. Penny was also instrumental in repositioning Finjan Software as a leading corporate-security provider, negotiating major contracts with IBM, Intel and Cisco. And she developed an aggressive product strategy that resulted in increased visibility and revenues for the computer security company Tripwire.

Bob Slapnik
Vice President of Government Sales
Bob Slapnik has a track record of successful sales management in Fortune 1000 and federal government accounts. He was president of Network Test Solutions, a channel sales organization serving the needs of network test labs with a wide range of tools for security and performance testing. He was President of Chesapeake Capital Corp. which arranged financing for commercial real estate and businesses. Bob has also held various sales and marketing positions with NetIQ, Antara, Sequent Computer Systems and Hewlett Packard. Bob has a Masters of Business Administration and a Bachelor of Science in Mathematics, both from Kent State University.

Company History

Company Timeline:

- **2003:** Founded as LLC to do consulting work for government agencies
- **2004:** Changed ownership structure to Subchapter S Corporation
- **September, 2005:** Received Phase 2 Small Business Innovation Research award from the United States Air Force
- **August, 2007:** Received Phase 2 Small Business Technology Transfer award from the United States Air Force
- **December 2007:** Received Phase 2 Small Business Technology Transfer award from the Department of Homeland Security
- **March 2008:** Released Responder line (Field and Pro)
- **March 2009:** Released Digital DNA and announced Digital DNA™ for McAfee's ePO
- **September 2009:** Released DDNA for ePO and made first two enterprise sales
- **March 2010:** Announced Active Defense™ and DDNA for Encase™ Enterprise
- **June 2010:** Released Active Defense

McAfee®

"In April 2010, the Romanian police announced the arrest of 70 members of three separate organized Cybercrime groups. Since 2006 these groups have allegedly stolen funds from citizens of Spain, Italy, France, New Zealand, Denmark, Sweden, Germany, Austria, the United States, Canada, and Switzerland primarily through online auction fraud. ***International authorities have identified more than 800 victims with more than €800,000 worth of losses****."*

"The criminals are said to have sold fictional electronic, luxury cars, yachts, villas, and even airplanes. Recent sales included a BMW X5, Lexus and Infiniti vehicles, and even a ***recreational aircraft that sold for €67,000 to a rich American****."*

Sources:
McAfee Threats Reports: Second Quarter 2010
Dicot, June 2010
Gandul, April 2010

Competitive Landscape

Yet to meet a true rival, HBGary competes with several other vendors in the threat detection and digital forensics marketplace. Competitor forensic software companies are focused on live forensics – the ability to monitor a computer as it runs and attempt to identify malicious code infections or security breaches that affect the disk. Also, competitor security software companies are using host intrusion detection systems (IDS) and anti-virus (AV) agents to limit malicious code infections and security breaches. However, HBGary provides the best of both worlds with a best-in-class product suite offering full forensics capabilities along with their extremely advanced defense technology. As a result, HBGary has yet to encounter a superior competitor.

Listed below is the detail competitive landscape relative to HBGary:

Competitors in Disk Forensics

- Access Data
- Westone - police and small business only
- Guidance Software (entropy is their "security" option)
- Mandiant's MIR
- Technology Pathways

Competitors in Memory Forensics

- Mandiant – with their offering of the free tool Memoryze
- Volatility

Competitors in Threat Detection - All Rely on Signatures

- McAfee
- Symantec
- Guidance's CyberSecurity Solution
- PrevX
- Any HIPS products
- Fireeye (perimeter only, based upon SNORT engine and still signature based)

Although other companies might enter this space, HBGary has a far greater potential to partner with these companies because the Company has four key differentiators that separate it from the competition.

- WPMA Technology analyzes physical memory offline and online
    - Analysis technique unique to HBGary
    - Offline is the most accurate way to detect advanced malicious code
- Digital DNA – identify any file in live memory
    - Technique unique to HBGary
    - Technique will revolutionize live malware detection engines
- Advanced Malware Detection
    - The HBGary baserules engine runs on physical memory images
    - Detection technique is unique to HBGary
- Malware Analysis Engine
    - Automated Malware Analysis
    - Runtime Malware Analysis

HBGary's products are in a class unto themselves in their capability to address the funded and state-sponsored threats that are utilizing new and unknown cyber weapons such as advanced attack tools, rootkits, stealth, and anti-forensics. The competition cannot address advanced attack tools and they are unable to collect evidence that can be used against attackers.

Active Defense is new to the market, but is gaining ground as an enterprise solution for the detection of advanced persistent threat and enterprise-wide incident response. This is competitive with both Guidance Software's *EnCase Enterprise* and Mandiant *MIR*, neither of which can detect unknown malware with comparable efficiency or accuracy. In addition, Active Defense is far more scalable and efficient when the enterprise has limited ability to transfer data within the network.

HBGary offers the leading technology for malware/advanced intrusion detection, follow-up incident response, remediation and inoculation. The Company's products are far superior to any competitors' solutions due to the fact that their products detect, disassemble, and asses malicious code better than any other vendor in the marketplace.

Financial Summary

	2006	2007	2008	2009	2010E*
Revenue					
Product Revenue	$387,500	$353,151	$1,030,442	$1,099,233	$2,349,281
Maintenance Revenue	$2,167	$13,183	$53,323	$166,660	$517,186
Digital DNA Annual Subscriptions	$0	$0	$0	$30,627	$199,224
Federal Government Revenue**	$628,982	$624,798	$690,790	$675,340	$97,805
Training and Consulting Revenue	$663,496	$897,547	$636,542	$1,008,194	$990,695
Total Revenue	$1,682,145	$1,888,679	$2,411,097	$2,980,054	$4,154,191
Total COGS	$723,525	$646,454	$533,059	$623,393	$340,068
Gross Profit	$958,620	$1,242,225	$1,878,038	$2,356,661	$3,814,123
Operating Expense					
Sales & Marketing	$112,054	$156,569	$494,335	$721,713	$938,524
Research & Development	$388,560	$358,528	$342,459	$435,278	$753,191
General & Administrative	$595,749	$821,914	$873,278	$879,766	$1,160,530
Total Operating Expenses	$1,096,363	$1,337,011	$1,710,071	$2,036,757	$2,852,246
Operating Profit	($137,743)	($94,786)	$167,967	$319,904	$961,877

* Actual through 9/30/2010

** Represents SBIR Grant providing funds for HBGary to build product prototypes for potential government purchase

Because HBGary's SBIR Grants are expiring shortly, the Company is shifting more of its efforts to the commercial sector after the U.S. Government has essentially helped fund their innovative R&D. As a result, overall company profitability is rising due to the decreasing contribution of these grants, which carry a maximum (government-mandated) profit of 10%.

To date, HBGary's growth is constrained only by its limited resources. HBGary provides a truly unique, highly valued offering demanded by organizations interested in securing its network and critical data. As a small, technology driven company, HBGary has not developed the infrastructure necessary to adequately sell into the current and future demand. The Company has few marketing resources and a very small sales team with limited reach and capacity. Despite these constraints, HBGary has experienced an overwhelming demand based on their superior product offering and unmatched reputation.

Inside a larger organization, there is no limit to HBGary's growth. Given the potential universal demand for the Company's products, a large security provider could achieve significant revenue almost immediately by exploiting available sales channels and offering HBGary's products to its existing customer base. In addition to simply selling HBGary's products to existing customers, an established firm could leverage its brand-name, strong customer relationships and reputation to extract greater value from customers during the sales process.

Glossary of Terms

- **Anti-virus Software** - used to prevent, detect, and remove malware, including computer viruses, worms, and trojan horses. Such programs may also prevent and remove adware, spyware, and other forms of malware.

- **Botnet** - collection of software agents, or robots, that run autonomously and automatically.

- **Checksums** - fixed-size datum computed from an arbitrary block of digital data for the purpose of detecting accidental errors that may have been introduced during its transmission or storage.

- **Computer Forensics** - the analysis of information contained within and created with computer systems and computing devices, typically in the interest of figuring out what happened, when it happened, how it happened, and who was involved.

- **Conficker –** computer worm targeting the Microsoft Windows operating system that was first detected in November 2008.

- **Developer Toolmarks** - unique traits left behind by the malware author.

- **GhostNet** - the name given by researchers at the Information Warfare Monitor to a large-scale cyber spying operation discovered in March 2009. Its command and control infrastructure is based mainly in the People's Republic of China and has infiltrated high-value political, economic and media locations in 103 countries.

- **Lexical Analysis** - process of converting a sequence of characters into a sequence of tokens.

- **Malware** - short for *malicious software*, is software designed to infiltrate a computer system without the owner's informed consent.

- **Obfuscated code** - source or machine code that has been made difficult to understand.

- **Opcode -** portion of a machine language instruction that specifies the operation to be performed. Their specification and format are laid out in the instruction set architecture of the processor in question.

- **Operation Aurora –** cyber attack which began in mid-2009 and continued through December 2009. The attack was first publicly disclosed by Google on January 12, 2010, in a blog post. In the blog post, Google said the attack originated in China.

- **Perimeter security** - set of physical security and programmatic security policies that provide levels of protection against remote malicious activity.

- **Phishing Attack** - criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication.

- **Random-access memory** (**RAM**) - form of computer data storage. Today, it takes the form of integrated circuits that allow stored data to be accessed in any order disk – based.

- **Regular Expressions** - provide a concise and flexible means for matching strings of text, such as particular characters, words, or patterns of characters.

- **Trojan horse** – malware that appears to perform a desirable function for the user prior to run or install but instead facilitates unauthorized access of the user's computer system

- **Zero-day exploits** - used or shared by attackers before the software developer knows about the vulnerability.

- **Zero-day malware - computer** threat that tries to exploit computer application vulnerabilities that are unknown to others or undisclosed to the software developer.

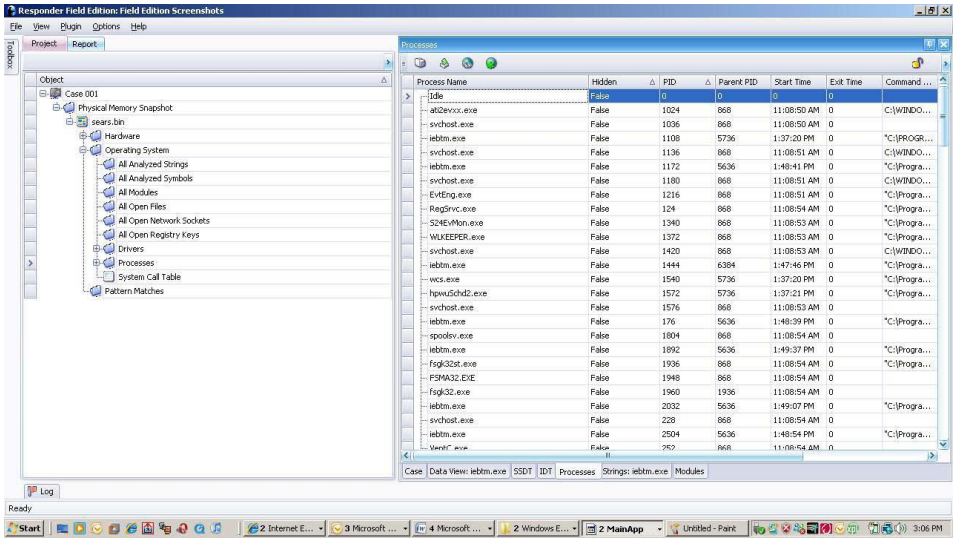
- **Zeus** - Trojan horse that steals banking information by keystroke logging. Zeus is spread mainly through drive-by downloads and phishing schemes.

Appendix 1: Product Descriptions

With HBGary's unique product suite consisting of the most sophisticated threat detection, malware and memory forensics solutions available, organizations can quickly gather critical evidence to contain the threat, locate compromised machines, and assess the damage. Considering all of HBGary's cutting-edge security software products, the Company provides the only solution that allows organizations to customize inoculation shots, remediate the malware problem, and prioritize malware in an efficient and easy to understand manner suitable for the average IT member.

Responder™ Field Edition

Responder Field Edition is a complete Windows Memory investigation suite. It is a necessary tool for all computer forensic investigators, law enforcement and information security professionals in order to capture and identify critical information found in memory.



Responder Professional

Responder Professional is the ultimate in Windows physical memory and automated malware analysis solution. Utilizing FDPro, this powerful tool is completely integrated into one application for great usability, streamlined workflow, and rapid results. The Professional platform is designed for incident responders, malware analysts, and computer forensic investigators who require rapid, effective, and accurate results.

Combined with Digital DNA, Responder Professional provides powerful memory forensics and malware identification. Malware analysis includes automated code disassembly, behavioral profiling reporting, pattern searching, code labeling, and control flow graphing - huge progression for the information security and computer forensic communities. Finally, these long-awaited capabilities are available to complement enterprise security best practices in the areas of host intrusion detection, computer forensics and security assessments.

Active Defense
Active Defense leverages existing infrastructure and the security team's skill set to maximize efficiency through the following the methods:

- Scalable Advanced Searching
    - Scan enterprise-wide for indicators of compromise within physical memory, physical NTFS drive volumes and from live operating system and registry.
- Unmatched Performance
    - Can scan thousands of end-nodes concurrently with minimal impact on network, which is very friendly to organizations unable to sustainably handle immense masses of data transfers.
    - Scans for registry keys or a known file in seconds. Powerful method for detecting which hosts have been compromised.
    - Scans of raw physical disk, thousands of patterns at once, 250GB per hour (4GB per minute sustained).
- Highly Accurate Threat Intelligence
    - Critical evidence can be extracted from the end node, revealing what tools were used, how the attacker moved laterally in the network, and what credentials have been compromised. Timeline information gathered from temporary Internet files, Pref-tech, and user registries can be used to determine an initial point of infection (IPI).
- Ease of Use
    - Active Defense's state-of-the-art analysis correlation engine provides reporting that can be easily used by your average IT team member. The user does not need to be an expert at reverse engineering or incident response to achieve unprecedented results. Most data presented is familiar to those trained in IT, such as process and module lists, file paths, registry keys, and URL paths. Low level technical information is presented largely as human-readable strings and is no more complicated than reading a packet-sniffer - a skill that most IT professionals possess.

FDPro™
FDPro is the commercially supported version of Fastdump. FDPro supports all versions of Windows operating systems and service packs (2000, XP, 2003, Vista, 2008 Server) 32 and 64 bit, including systems with more than 4 GBs of RAM and up to 64 GBs of RAM. The product also supports acquisition of the Windows page file to be included with RAM, while also supporting a variety of memory probing features that assist with malware analysis.

HBGary Health Check
With HBGary Health Check, the Company closes the gap between traditional digital security technologies and proactive security solutions. Due to the ever-changing and sophisticated nature of present day malware, the safety of the end node can no longer be secured by sole reliance upon perimeter security, network traffic analysis, or anti-virus systems. To combat these problems, HBGary provides a comprehensive data security health check, at the end node, to detect previously undiscovered and dangerous malware that is penetrating, embedding, and executing on any given system.

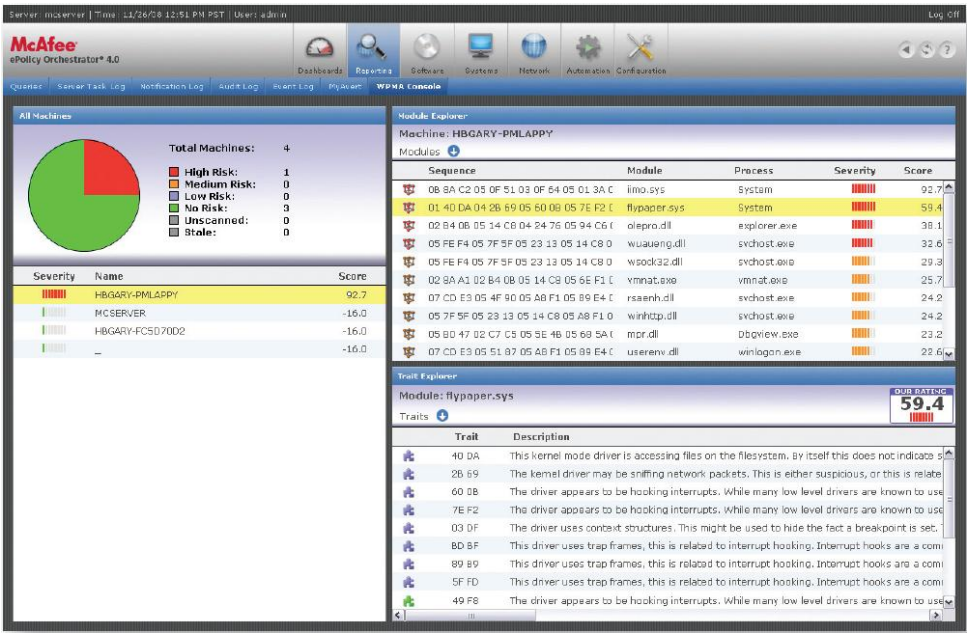
Appendix 2: Technology Description

Forensically-Sound Technology
All HBGary technology is forensically-sound.

"A 'forensically-sound' duplicate of a drive is, first and foremost, one created by a method which does not, in any way, alter any data on the drive being duplicated. Second, a forensically-sound duplicate must contain a copy of every bit, byte and sector of the source drive, including unallocated 'empty' space and slack space; precisely as such data appears on the source drive relative to the other data on the drive. Finally, a forensically-sound duplicate will not contain any data (except known filler characters) other than which was copied from the source drive."

HBGary Digital DNA™ for McAfee ePolicy Orchestrator®
McAfee users can deploy Digital DNA on top of existing ePO enterprise infrastructure, increasing value derived from current hardware, software, and network communications. No new host agents are required. Installing and scheduling Digital DNA are handled by ePO. The user can use Digital DNA with little or no training to gain endpoint security visibility. Malware threats are automatically displayed on the web-based ePO dashboard console. Behavioral traits provide quick threat metadata. Historical alerts are centrally reported and correlated. HBGary participates in the McAfee Security Innovation Alliance partner program.

Strongly applicable across several verticals, HBGary's Digital DNA technology is currently being used by consulting firms, financial firms, government agencies, the DoD, and entertainment, high technology and pharmaceutical firms.



Supported Operating Systems

- Windows® 2000
- Windows® 2003 Server
- Windows® 2008 Server
- Windows® XP
- Windows® Vista
- Windows® 7

HBGary Digital DNA™ Enterprise

HBGary Digital DNA Enterprise allows customers to perform physical memory analysis of remote Windows computers from a central location. Malware alerts, suspicious programs, data and memory images are archived and managed within the HBGary Evidence Server and Console. Digital DNA software can be deployed to host endpoints either as an agent running as a service or as a command line utility, giving you deployment flexibility. Flexible licensing allows you to deploy Digital DNA reactively to targeted computers or proactively for the entire enterprise.

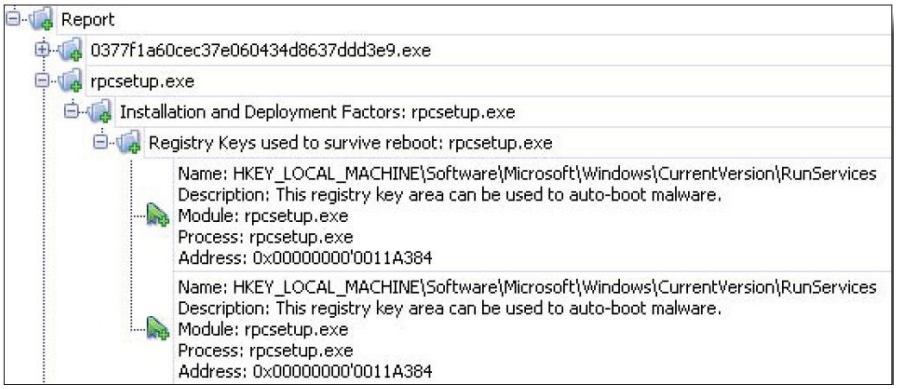
Automated Malware Analysis

More and more computer crimes have been perpetrated with malware utilized as the method of gaining access to confidential information. The new face of malware is designed to never touch the disk and reside only in memory. Responder provides easy to use "runtime information" to identify rootkits and malware not detected by anti-virus.

Process Name	... △	Command Line	Start Time
Idle	0		0
rpcsetup.exe	1012	"C:\Program Files\Access Remote PC 4\rpcsetup.exe" /server /silent	4:33:06 PM
iexplore.exe	1040	"C:\Program Files\Internet Explorer\iexplore.exe"	12:00:15 ...
VMwareService.e	1088	"C:\Program Files\VMware\VMware Tools\VMwareService.exe"	4:33:06 PM
procexp.exe	1236	"C:\toolz\procexpnt\procexp.exe"	12:00:06 ...
cmd.exe	1244	"C:\WINDOWS\system32\cmd.exe"	12:00:11 ...
explorer.exe	1512	C:\WINDOWS\Explorer.EXE	4:33:09 PM

Critical computer artifacts are found only in live memory and Responder makes it easy to uncover and take advantage of this search, identify and report critical information with easy to use and an intuitive graphical user interface (GUI) designed to support investigation workflow.

User Interface and Reporting: Responder has a friendly user interface to support investigator workflow. A flexible reporting module allows quick delivery of information to attorneys, management or clients. Reports can be exported out to CVS, PDF, RTF and other reporting standards.

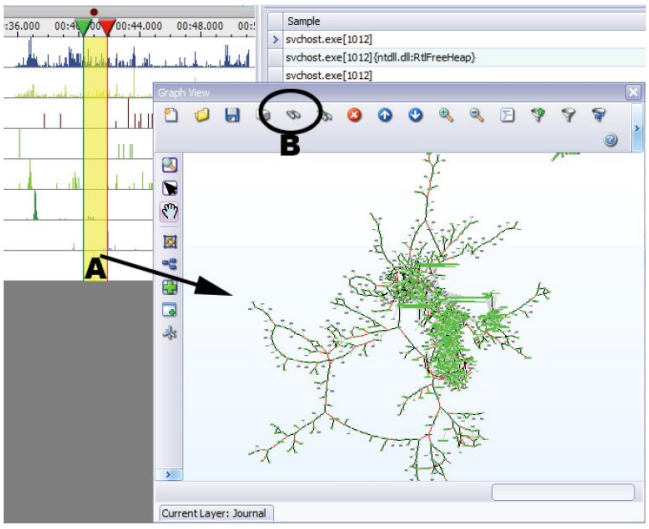


REcon™

REcon performance outclasses everything currently available in the market, operating orders of magnitude faster than any other known tracing solutions. REcon high performance allows users to interact with a program's graphical user interface (GUI) while also single-step recording every instruction in that program – something that has never been possible with prior technology. REcon supports advanced performance features when on native hardware, such as the use of the branch-trace mode on Intel processers.

REcon can record the entire lifecycle of a software program, from the first instruction to the last. All behavior is recorded, including all loaded DLLs, plug-ins, browser helper objects (BHOs), file system activity, network activity, and registry access. Users can configure additional tracks of data to be recorded with almost limitless ways. Any function point can be recorded; including DLL exported functions, and internal undocumented functions (API-spy type capability). Users can control the sampling behavior, including number and type of arguments to a call.

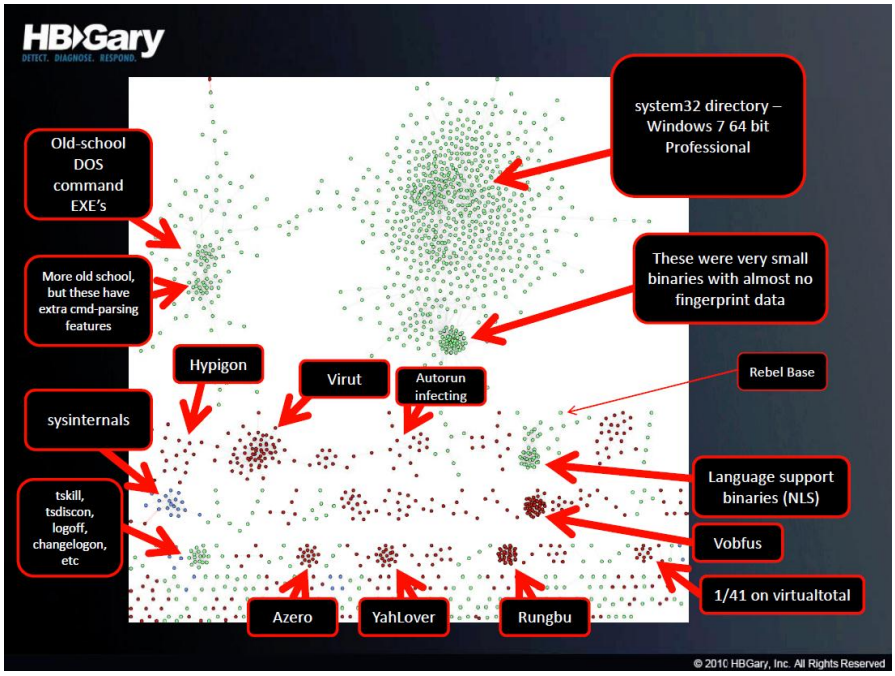
The full control flow graph is recovered for a program, including all basic blocks and branch conditions, even branches not taken. The opcodes, top of stack, and register context can be captured at a single-step resolution. This allows the recovery of packed executables, such as those packed by ASProtect, ASPack, Armadillo, UPX, and even Themida. REcon operates entirely in kernel mode and remains hidden from many anti-debugger checks, including checks for kernel mode debuggers.



Beyond the recording capabilities, the data itself can be graphed and replayed in HBGary Responder Professional. A new track-control has been added to the graph that allows the user to interact with the recorded program timeline similar to the way they might interact with a recorded video or audio track. The user can graph individual tracks of behavior (such as networking), or they can graph just regions of behavior (such as only the decryption routine). Any region that can be graphed can also be placed into a separate layer and managed independently. All of the existing graph features that users have come to expect from Responder Professional can also be applied to any recorded track of behavior, thus exposing an entirely new set of data that will augment existing analysis.

HBGary's technology also provides the powerful ability to collect and cluster a large number of samples into groups of self-similar items. This feature enables the user to perform link analysis into social cyberspace to the participants behind the malware.

In other words, each dot is a different piece of malware. The malware clusters in groups based on the similar identified traits from the code base. Because each malicious code is uniquely developed and effectively linked to the developer, these clustered groups identify a different hacker. Thus, HBGary's technology links all identified malware back to the original source through a proficient, effective, accurate, and scalable manner that has never before been developed prior to the inception HBGary's groundbreaking technology.



HBGary
DETECT. DIAGNOSE. RESPOND.

Continuous Protection

HBGary
DETECT. DIAGNOSE. RESPOND.

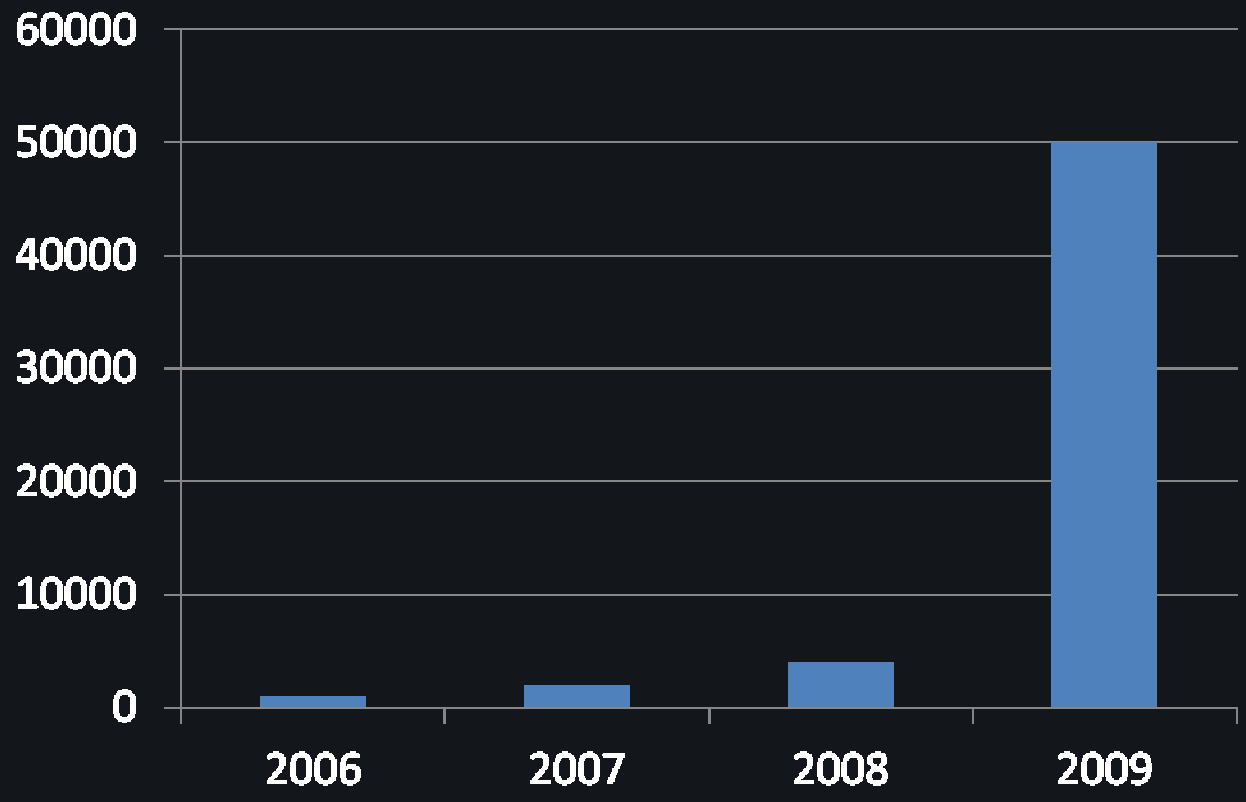
The Evolved Risk Environment

All data is digital and can be stolen by motivated and well funded attackers from 3,000 miles away. They are entrenched already.

Host-level protection is incomplete. Antivirus does not detect emerging threats. The host is highly vulnerable and this is where the bad guy gets in.

HBGary
DETECT. DIAGNOSE. RESPOND.

Signature based systems don't scale



HBGary
DETECT. DIAGNOSE. RESPOND.

There is NO RISK REDUCTION

- Incident Response & Reimage is the traditional model – but….
- Reimaging doesn't fix the vulnerability - over 50% of reimaged machines will end up re-infected with the same malware
- After the IR team leaves, the bad guys come crawling back out of their holes using multiple layers of entrenched malware and sleeper agents (hey, remember, these guys are *hackers*)

HBGary
DETECT. DIAGNOSE. RESPOND.

Continuous Protection

- The bad guys are going to get in. Accept it.
- Because intruders are always present, you need to have a continuous countering force to detect and remove them.
- Your continuous protection solution needs to get smarter over time – it must learn how the attackers work and get better at detecting them. Security is an intelligence problem.

HBGary
DETECT. DIAGNOSE. RESPOND.

Efficient & Scalable Visibility

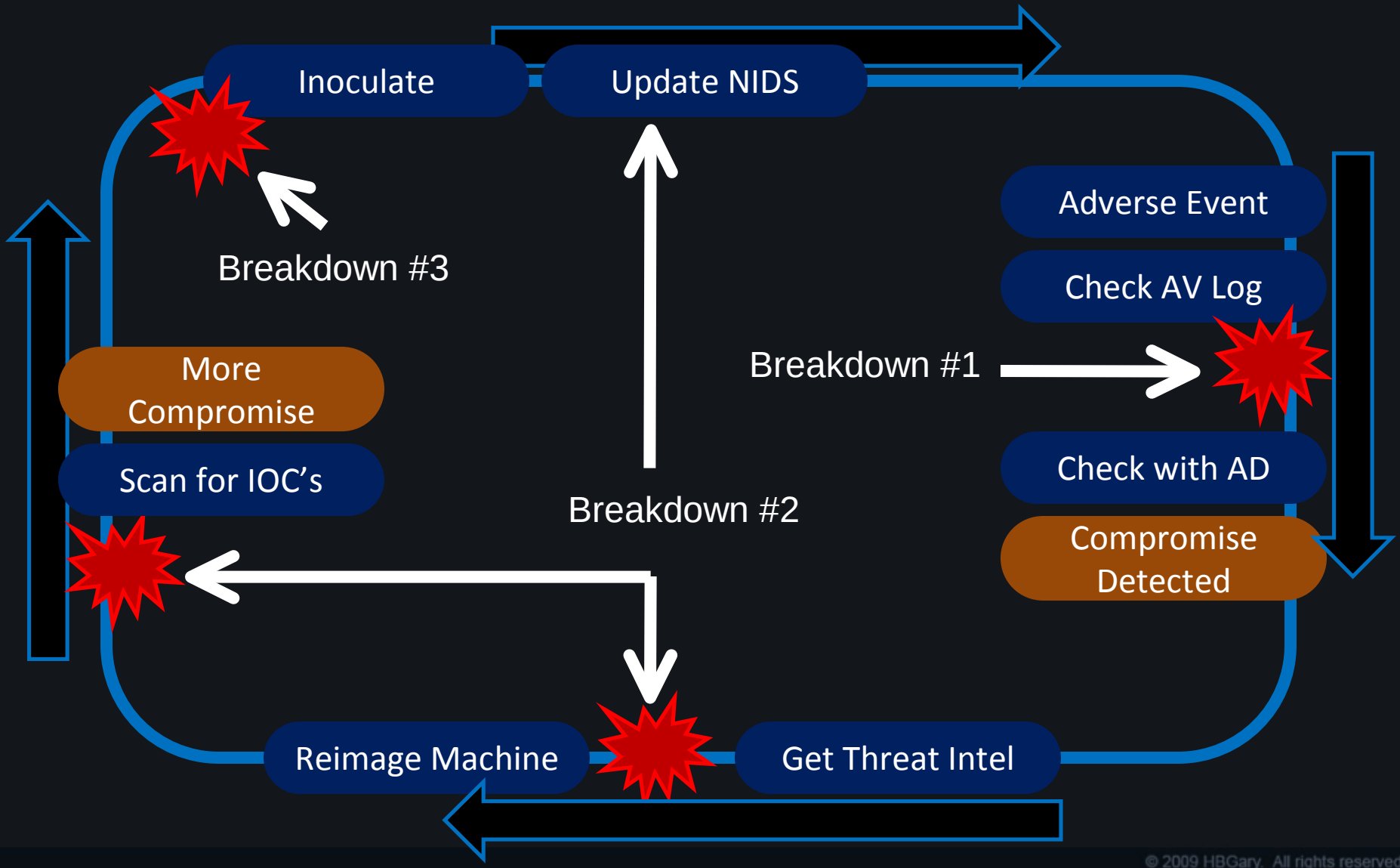
- To detect advanced intruders, the IR team needs whole-host remote live-forensics at the click of a button
- To be efficient, the team needs to search over tens of thousands of machines in minutes
- The solution needs to support all levels of analysis, from simple search to low-level disassembly

Countermeasures

- Once compromise is detected, data needs to be extracted that can be used for better intrusion detection
  - Registry keys, emails, DNS names, URL's, binary file signatures, in-memory signatures, etc.
- At all times, you need to think about how you will detect the attacker NEXT WEEK.

HBGary
DETECT. DIAGNOSE. RESPOND.

Continuous Protection



HBGary
DETECT. DIAGNOSE. RESPOND.

The Breakdowns

- #1 – Trusting the AV
  - AV doesn't detect most malware, even variants of malware that it's supposed to detect
- #2 – Not using threat intelligence
  - The only way to get better at detecting intrusion is to learn how to detect them next time
- #3 – Not preventing re-infection
  - If you don't harden your network then you are just throwing money away

HBGary
DETECT. DIAGNOSE. RESPOND.

The Big Picture of HBGary

- Detect bad guys using a smallish genome of behaviors – and this means zeroday and APT – no signatures required
- Followup with strong incident response technology, enterprise scalable
- Back this with very low level & sophisticated deep-dive capability for attribution and forensics work

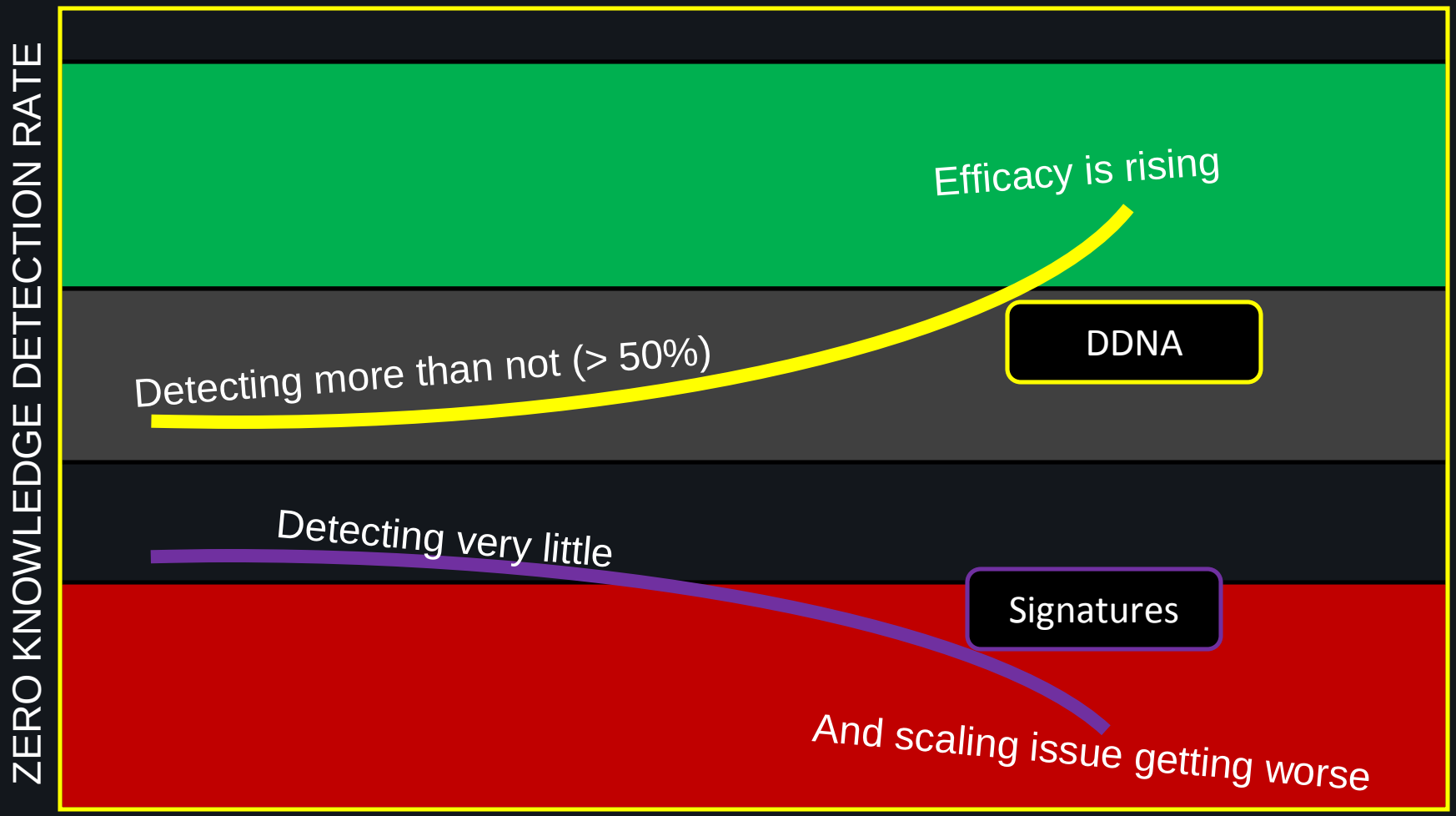
HBGary
DETECT. DIAGNOSE. RESPOND.

HBGary's take on all this

- Focus on malicious behavior, not signatures
  - There are only so many ways to do something bad on a Windows machine
- Bad guys don't write 50,000 new malware every morning
  - Their techniques, algorithms, and protocols stay the same, day in day out
- Once executing in physical memory, the software is just software
  - Physmem is the best information source available

HBGary
DETECT. DIAGNOSE. RESPOND.

Efficacy Curve



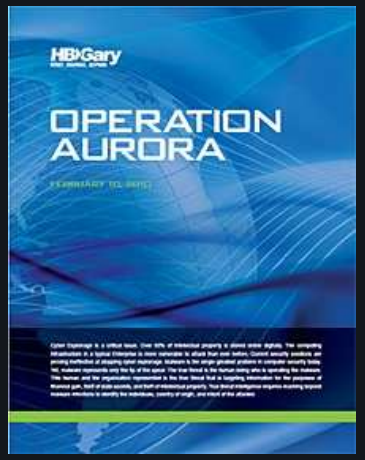
HBGary
DETECT. DIAGNOSE. RESPOND.

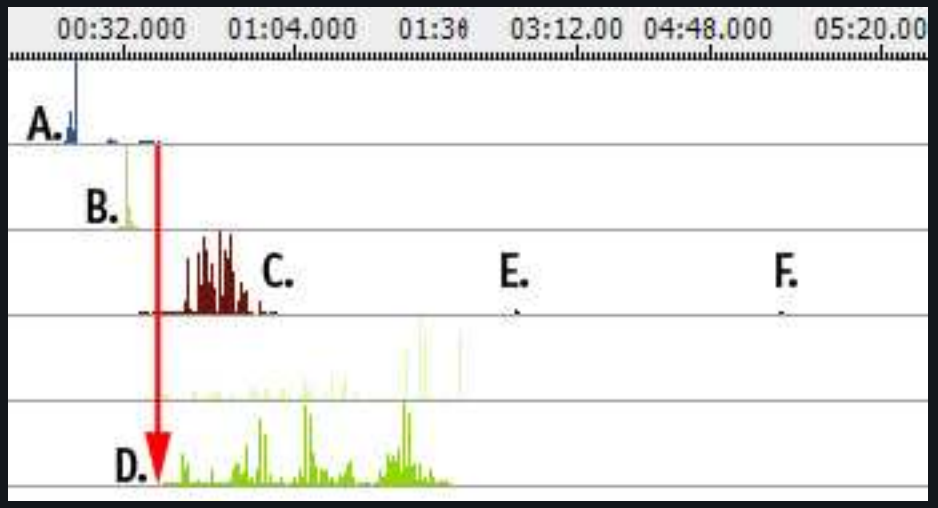
And The Very Near Future

- Digital Antibodies, deployed persistent protection against specific threat patterns
  - This only works for known malware or attack patterns
  - This causes the attacker's methods to stop working and limits their movement, forcing them to spend resources to maintain access

HBGary
DETECT. DIAGNOSE. RESPOND.

Inoculation Example





Using Responder + REcon, HBGary was able to trace Aurora malware and obtain actionable intel in about 5 minutes.

This intel was then used to create an inoculation shot, downloaded over 10,000 times over a few days time.

```
To automatically attempt a clean operation:
*******************************************

InoculateAurora.exe -range 192.168.0.1 192.168.0.254 -clean
```

HBGary
DETECT. DIAGNOSE. RESPOND.

Products

HBGary
DETECT. DIAGNOSE. RESPOND.

	Stand Alone	Enterprise
Memory Forensics	Responder Field Edition	Integrated with EnCase Enterprise (Guidance)
Enterprise Malware Detection		Digital DNA for ePO (HBSS)
		Active Defense
Response	Responder Professional w/ Digital DNA	*Intrinsic to all Enterprise products*
Policy Enforcement and Mitigation		Integrated with Verdasys Digital Guardian

HBGary
DETECT. DIAGNOSE. RESPOND.

Customers

DoD	26000 Nodes
Civilian Agencies	36,000 Nodes
Government Contractors & Consulting	44 Customers
OEMS	2
Fortune 500	52 Customers *
Foreign Governments & Customers	38
Universities & Law Enforcement	87 Customers

* Multiple site license discussions in the pipeline

HBGary
DETECT. DIAGNOSE. RESPOND.

Managed Service

HBGary
DETECT. DIAGNOSE. RESPOND.

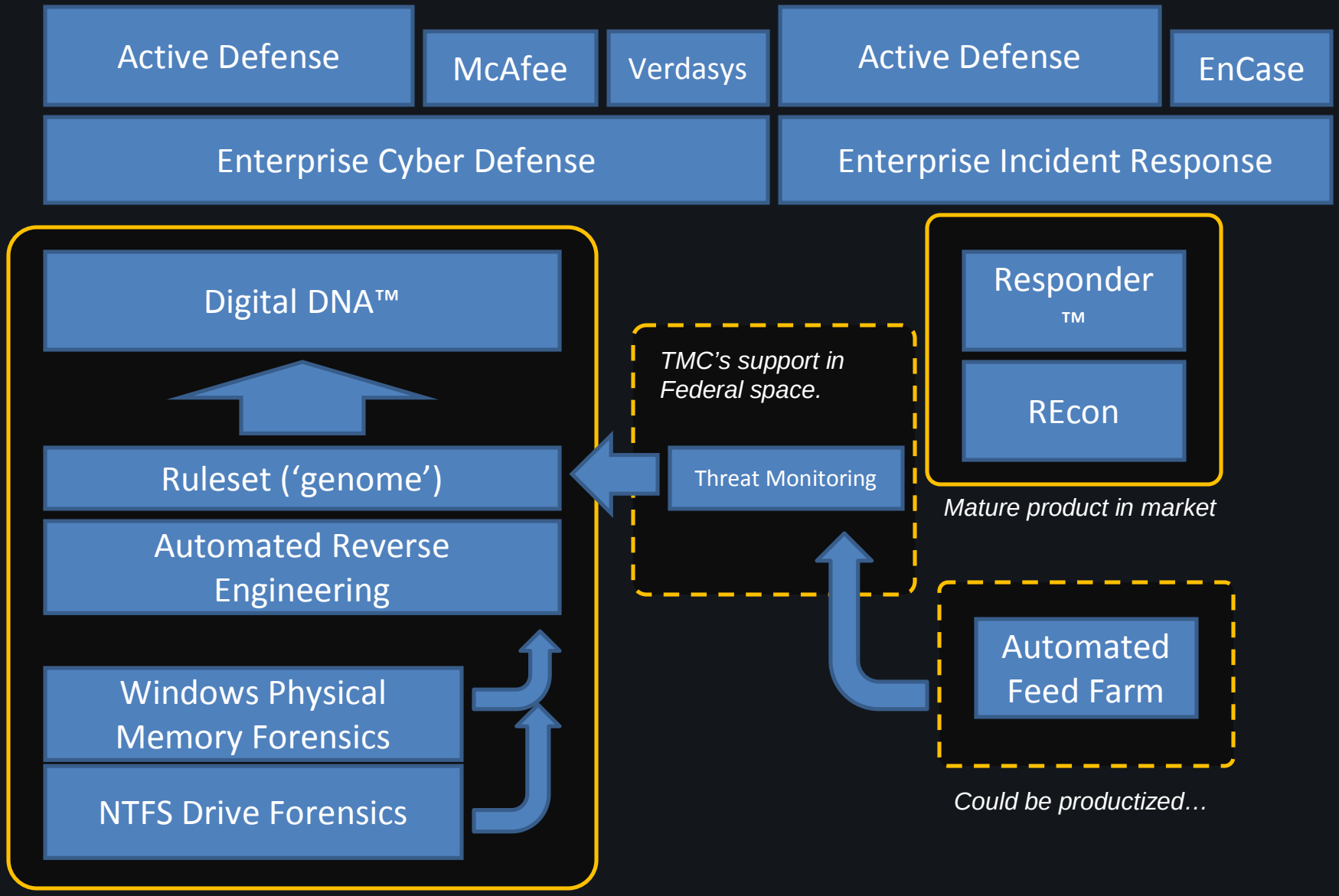
Managed Service

- Weekly, enterprise-wide scanning with DDNA & updated IOC's (using HBGary Product)
- Includes extraction of threat-intelligence from compromised systems and malware
- Includes creation of new IDS signatures
- Includes inoculation shot development
- Includes option for network monitoring specifically for C2 traffic and exfiltration

HBGary
DETECT. DIAGNOSE. RESPOND.

Technology Block Diagram

HBGary
DETECT. DIAGNOSE. RESPOND.



HBGary
DETECT. DIAGNOSE. RESPOND.

Digital DNA™

HBGary
DETECT. DIAGNOSE. RESPOND.

Digital DNA™

- **Automated** malware detection
- Software classification system
- 5000 software and malware behavioral traits
- Example
  - Huge number of key logger variants in the wild
  - About 10 logical ways to build a key logger

HBGary
DETECT. DIAGNOSE. RESPOND.

Digital DNA™ Benefits

- Enterprise detection of *zero-day* threats
- Lowers the skill required for actionable response
  - What files, keys, and methods used for infection
  - What URL's, addresses, protocols, ports
- "At a glance" threat assessment
  - What does it steal? Keystrokes? Bank Information? Word documents and powerpoints?

= Better cyber defense

HBGary
DETECT. DIAGNOSE. RESPOND.

How an AV vendor can use DDNA

- Digital DNA uses a smallish genome file (a few hundred K) to detect ***ALL*** threats
- If something is detected as suspicious, that object can be extracted from the surrounding memory (Active Defense™ does this already)
- The sample can then be analyzed with a larger, more complete virus database for known-threat identification
- If a known threat is not identified, the sample can be sent to the AV vendor automatically

HBGary
DETECT. DIAGNOSE. RESPOND.

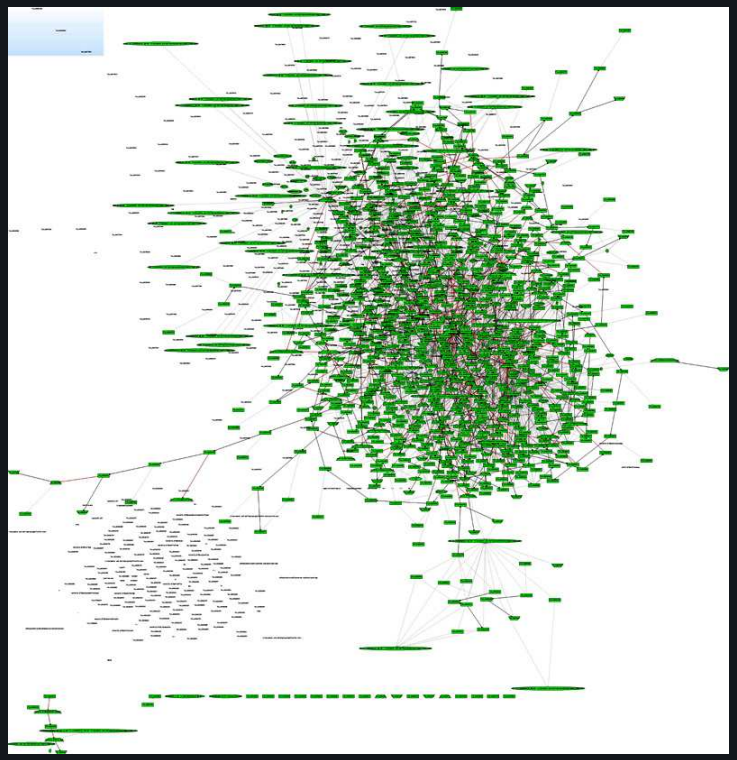
Digital DNA™ Performance

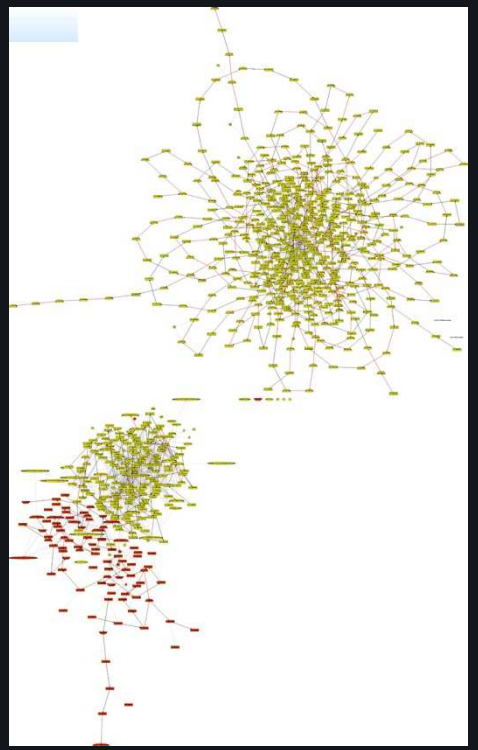
- 4 gigs per minute, thousands of patterns in parallel, NTFS raw disk, end node
- 2 gig memory, 5 minute scan, end node
- Hi/Med/Low throttle
- = 10,000 machine scan completes in < 1 hour

HBGary
DETECT. DIAGNOSE. RESPOND.

Under the hood

These images show the volume of decompiled information produced by the DDNA engine. Both malware use stealth to hide on the system. To DDNA, they read like an open book.





HBGary
DETECT. DIAGNOSE. RESPOND.

Digital DNA™

Ranking Software Modules by Threat Severity

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

0B 8A C2 05 0F 51 03 0F 64 27 27 7B ED 06 19 42 00 C2 02 21 3D 00 63 02 21

8A C2

0F 51

0F 64

Software Behavioral Traits

Trait

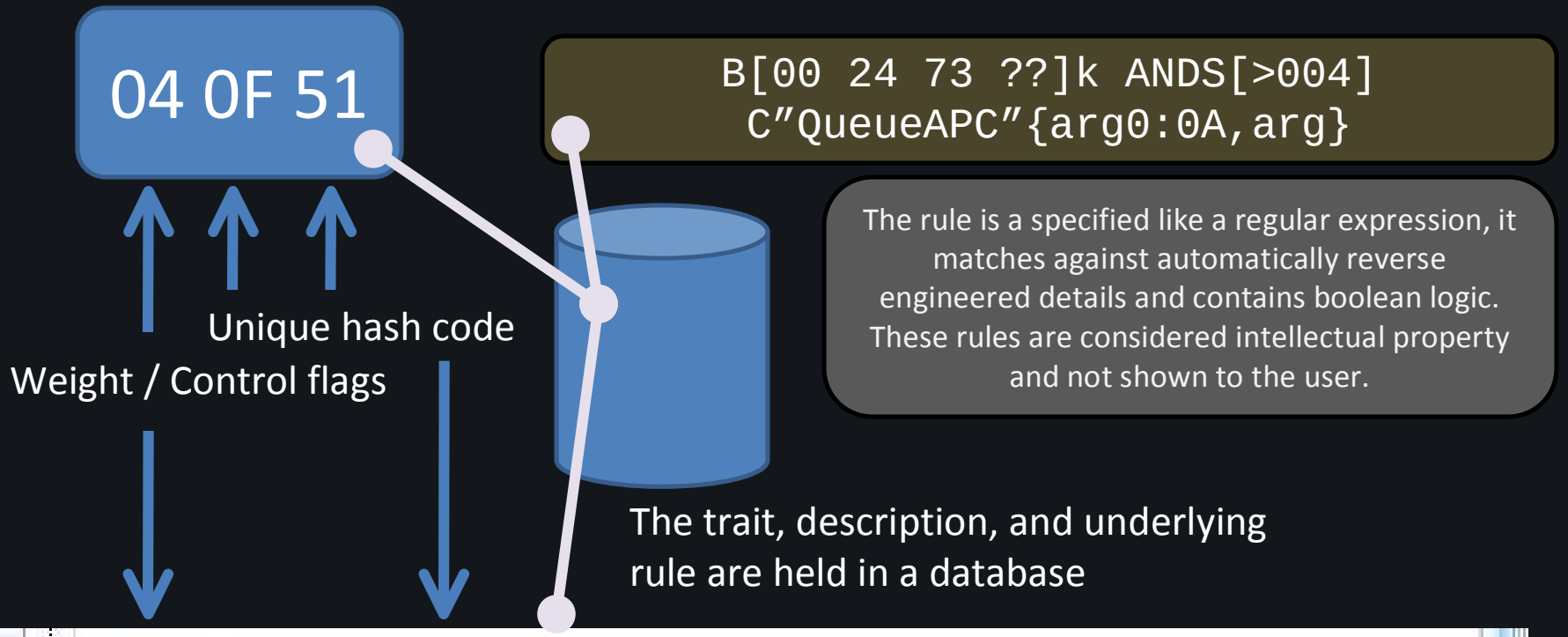
Trait: 8A C2
Description: The driver may be a rootkit or anti-rootkit tool. It should be examined in more detail.

Trait: 0F 51
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.

Trait: 0F 64
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.

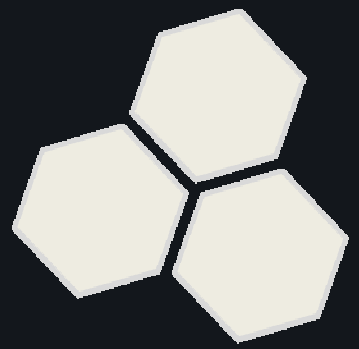
HBGary
DETECT. DIAGNOSE. RESPOND.

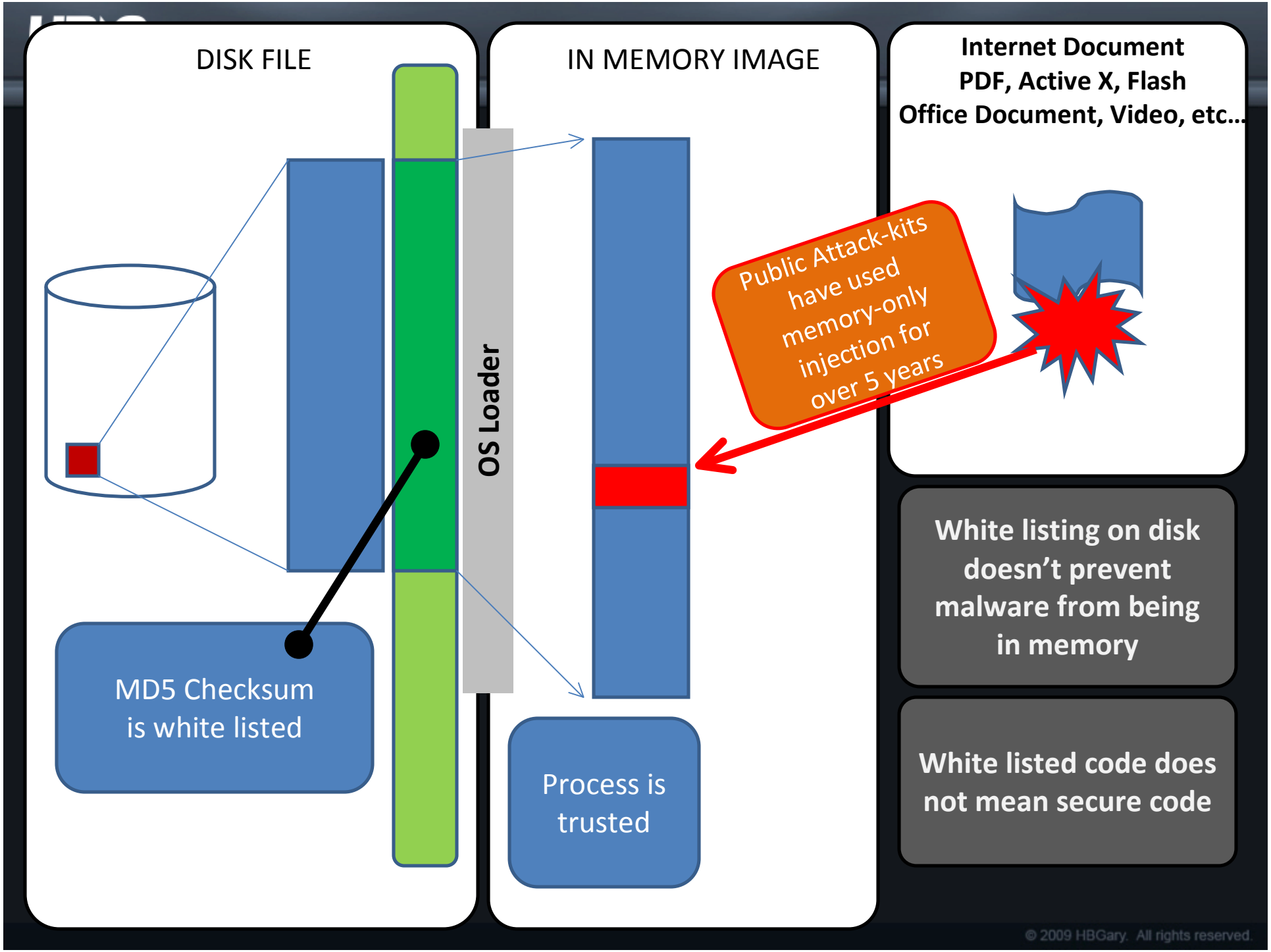
What's in a Trait?



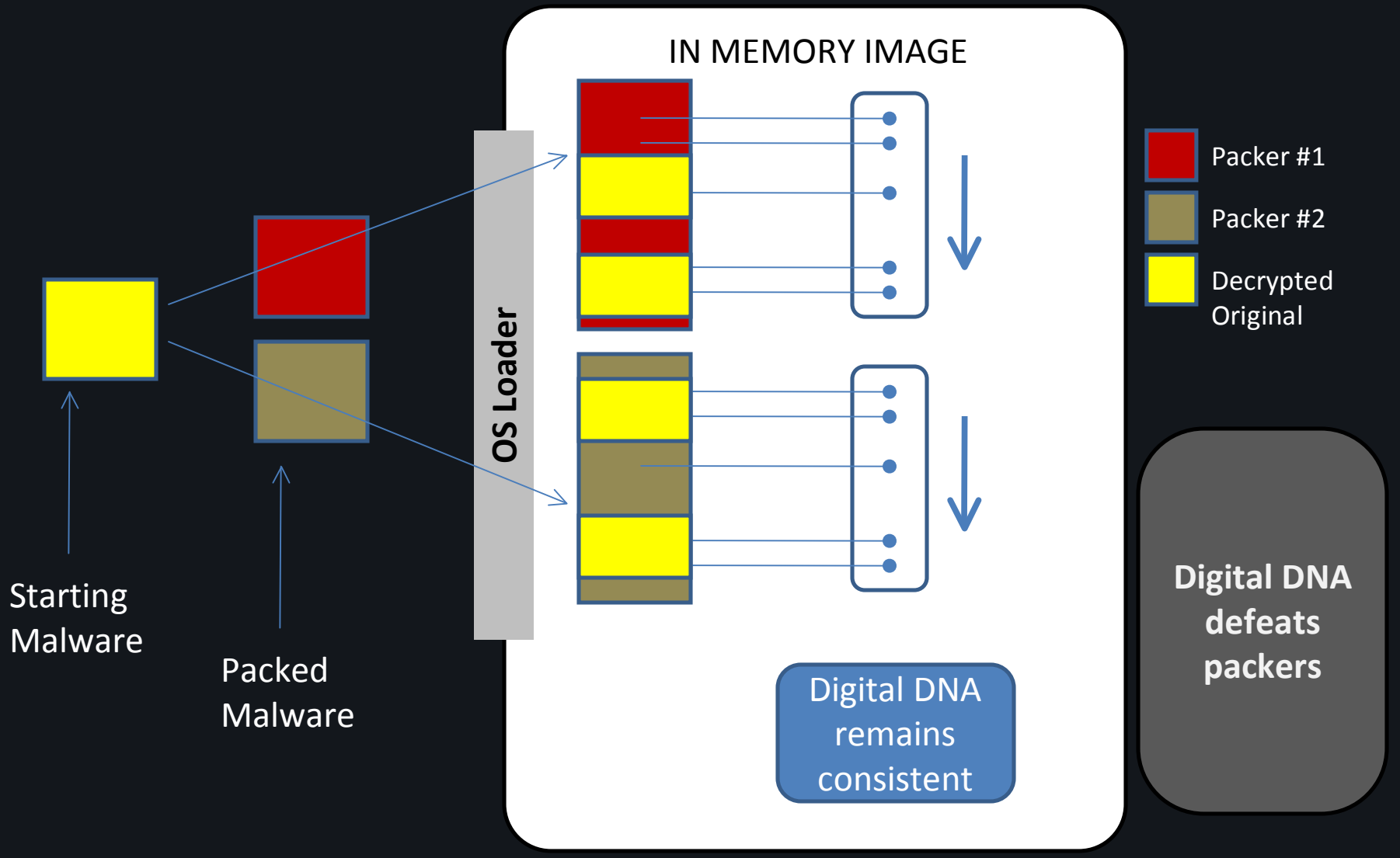
HBGary
DETECT. DIAGNOSE. RESPOND.

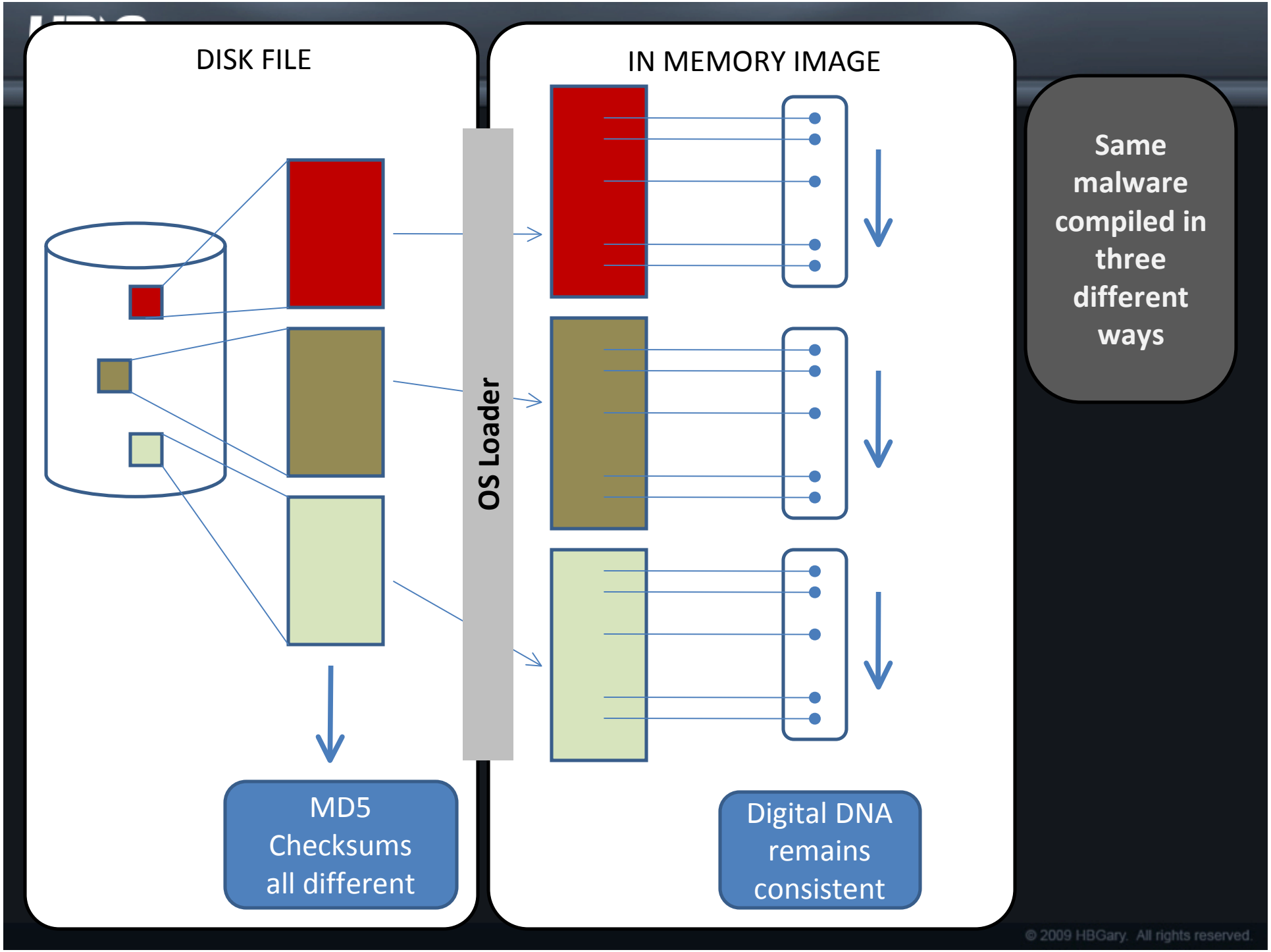
Digital DNA™ (in Memory)
vs.
Disk Based Hashing, Signatures, and other schematic approaches





HBGary
DETECT. DIAGNOSE. RESPOND.

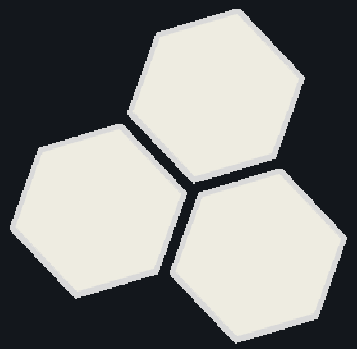




HBGary
DETECT. DIAGNOSE. RESPOND.

Compromised computers…

Now what?

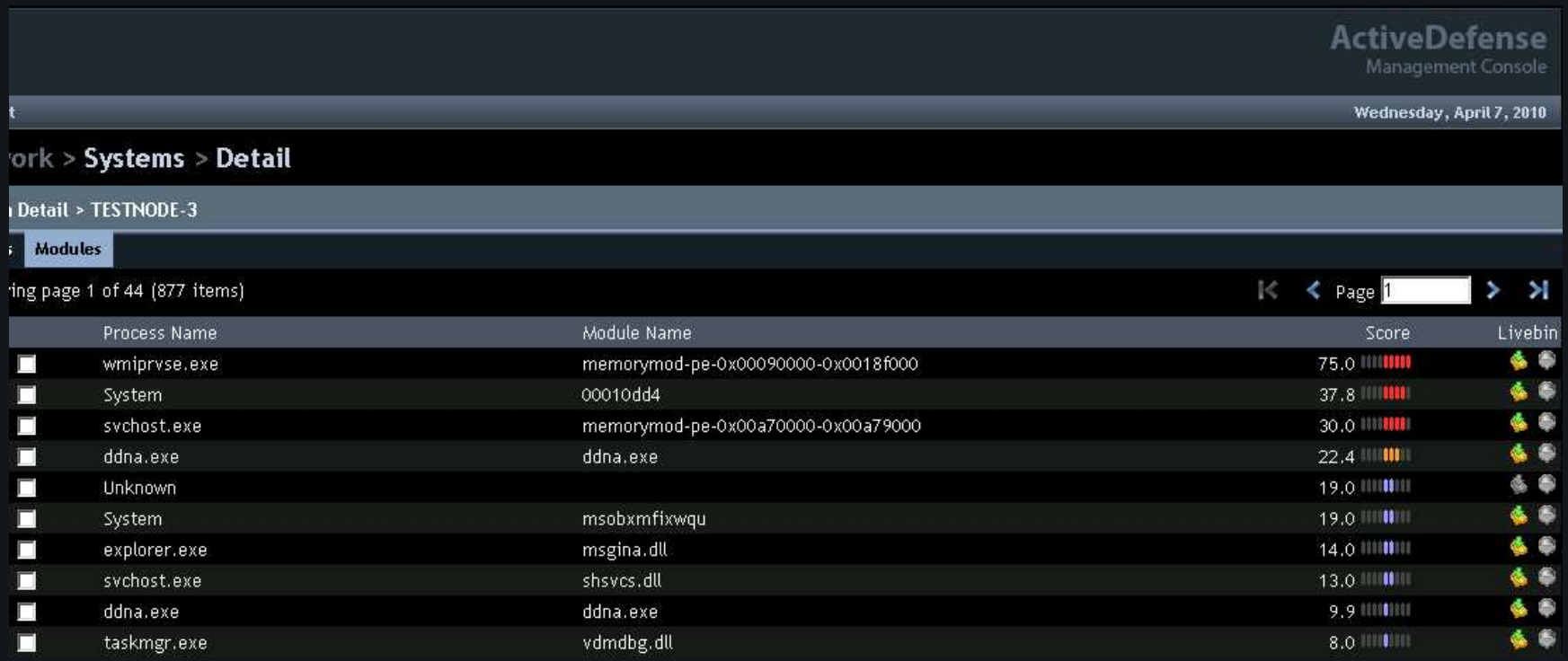


HBGary
DETECT. DIAGNOSE. RESPOND.

Active Defense™

HBGary
DETECT. DIAGNOSE. RESPOND.

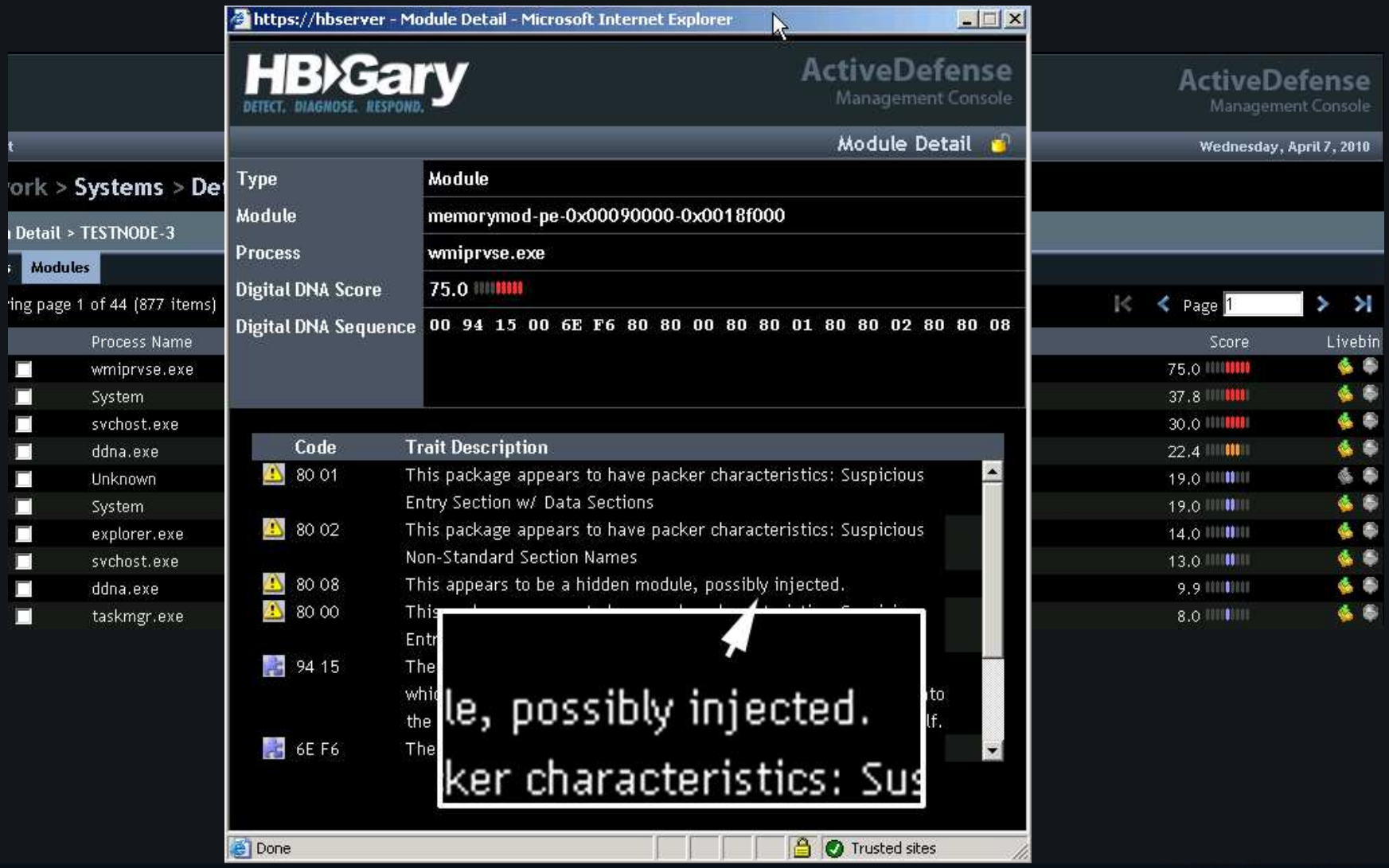
Alert!



Process Name	Module Name	Score	Livebin
wmiprvse.exe	memorymod-pe-0x00090000-0x0018f000	75.0	
System	00010dd4	37.8	
svchost.exe	memorymod-pe-0x00a70000-0x00a79000	30.0	
ddna.exe	ddna.exe	22.4	
Unknown		19.0	
System	msobxmfixwqu	19.0	
explorer.exe	msgina.dll	14.0	
svchost.exe	shsvcs.dll	13.0	
ddna.exe	ddna.exe	9.9	
taskmgr.exe	vdmdbg.dll	8.0	

HBGary
DETECT. DIAGNOSE. RESPOND.

Hmm..



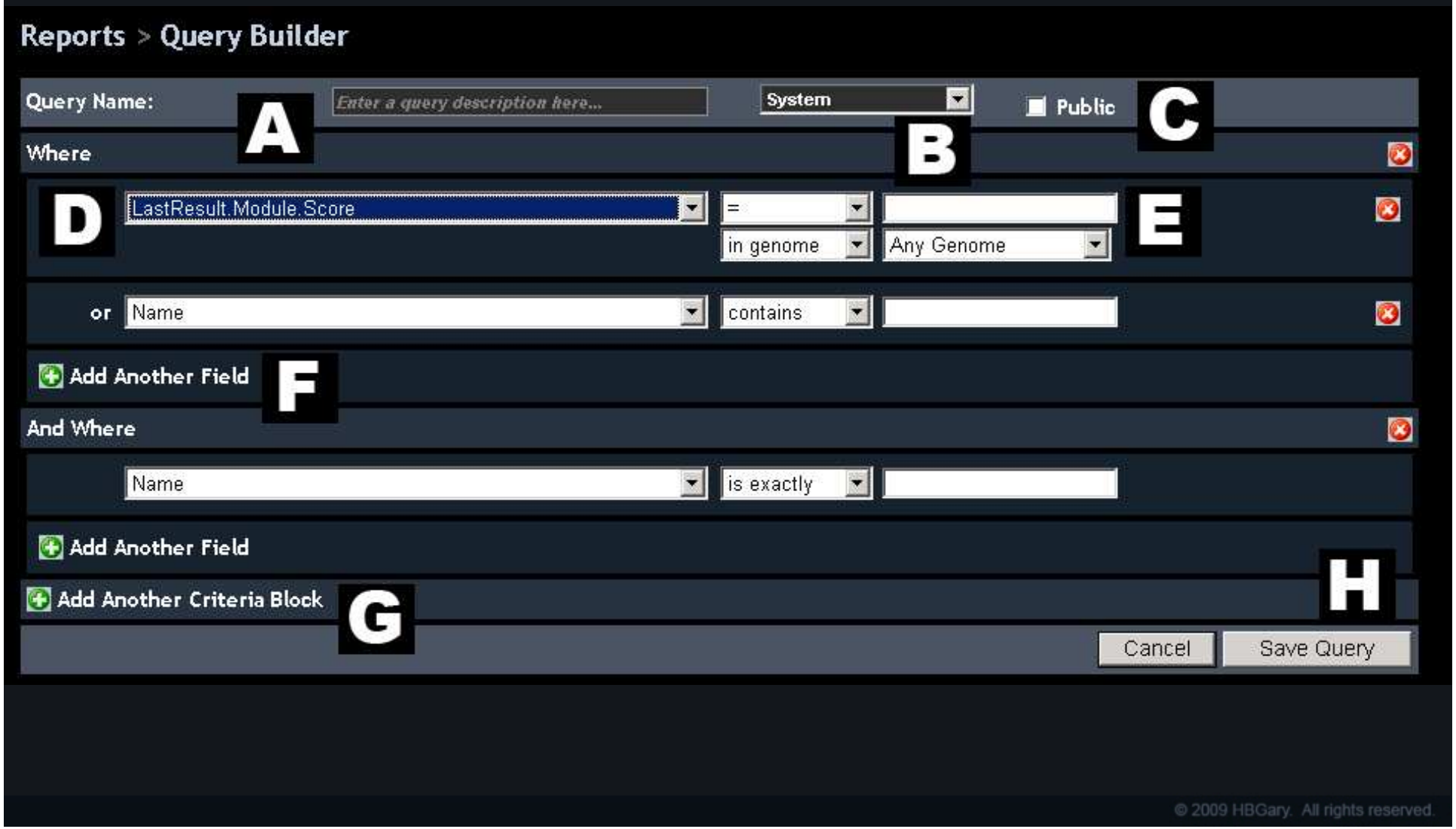
HBGary
DETECT. DIAGNOSE. RESPOND.

Active Defense Queries

- What happened?
- What is being stolen?
- How did it happen?
- Who is behind it?
- How do I bolster network defenses?

HBGary
DETECT. DIAGNOSE. RESPOND.

Active Defense Queries



HBGary
DETECT. DIAGNOSE. RESPOND.

Active Defense Queries

QUERY: “detect use of password hash dumping”

Physmem.BinaryData **CONTAINS PATTERN** “ No NDA no Pattern…☺ “

QUERY: “detect deleted rootkit”

(RawVolume.File.Name **=** “mssrv.sys“ **OR** RawVolume.File.Name = “acxts.sys“)
AND RawVolume.File.Deleted **=** TRUE

QUERY: “detect chinese password stealer”
LiveOS.Process.BinaryData **CONTAINS PATTERN** “LogonType: %s-%s“

QUERY: “detect malware infection san diego”
LiveOS.Module.BinaryData **CONTAINS PATTERN** “.aspack“ **OFFSET < 1024**
OR
RawVolume.File.BinaryData **CONTAINS PATTERN** “.aspack“ **OFFSET < 1024**

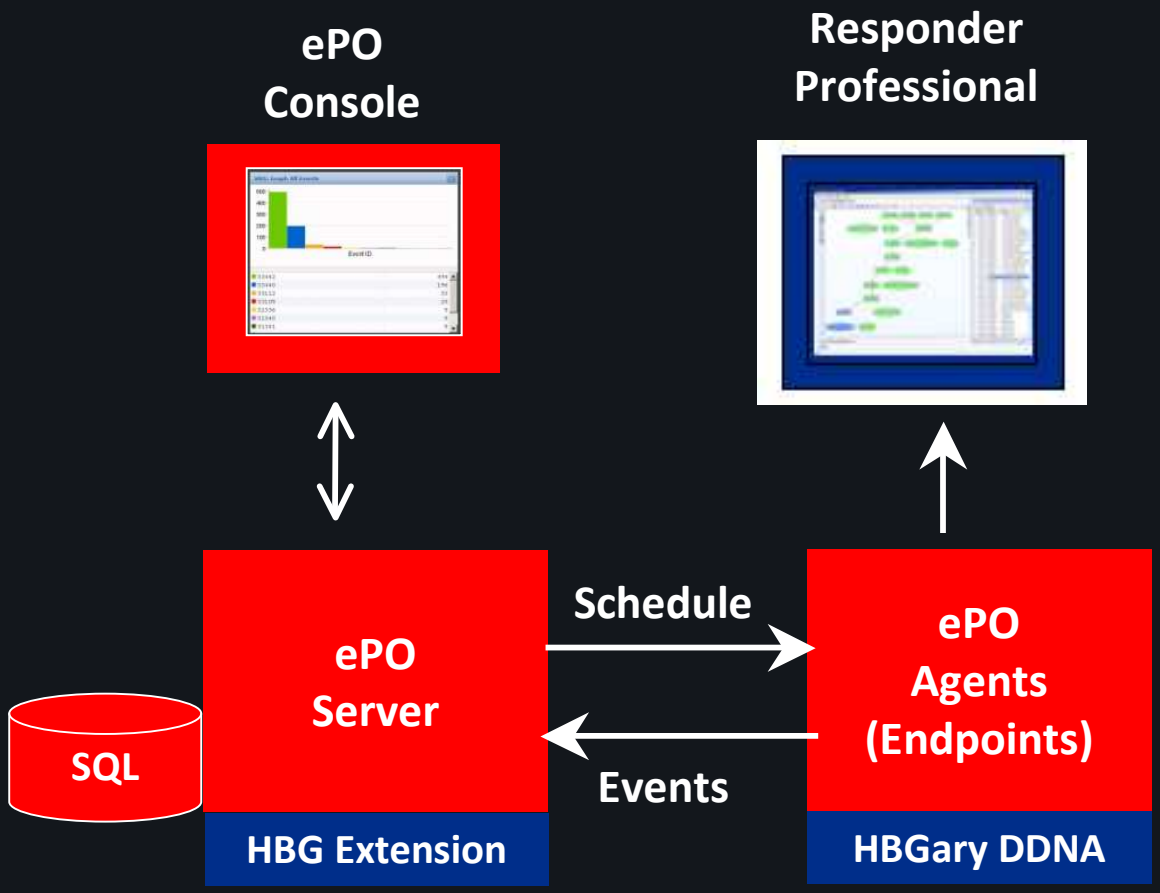
HBGary
DETECT. DIAGNOSE. RESPOND.

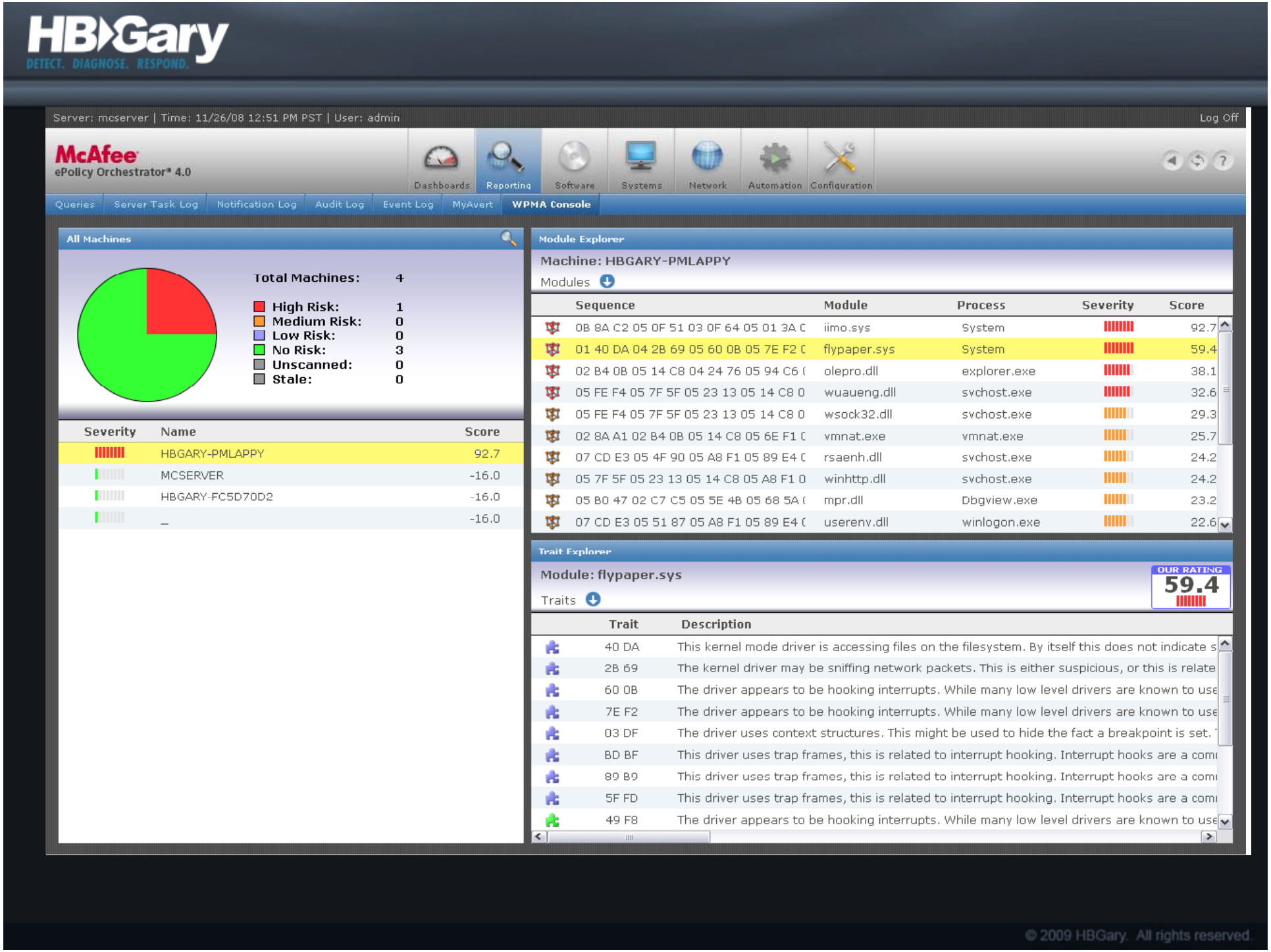
Enterprise Systems

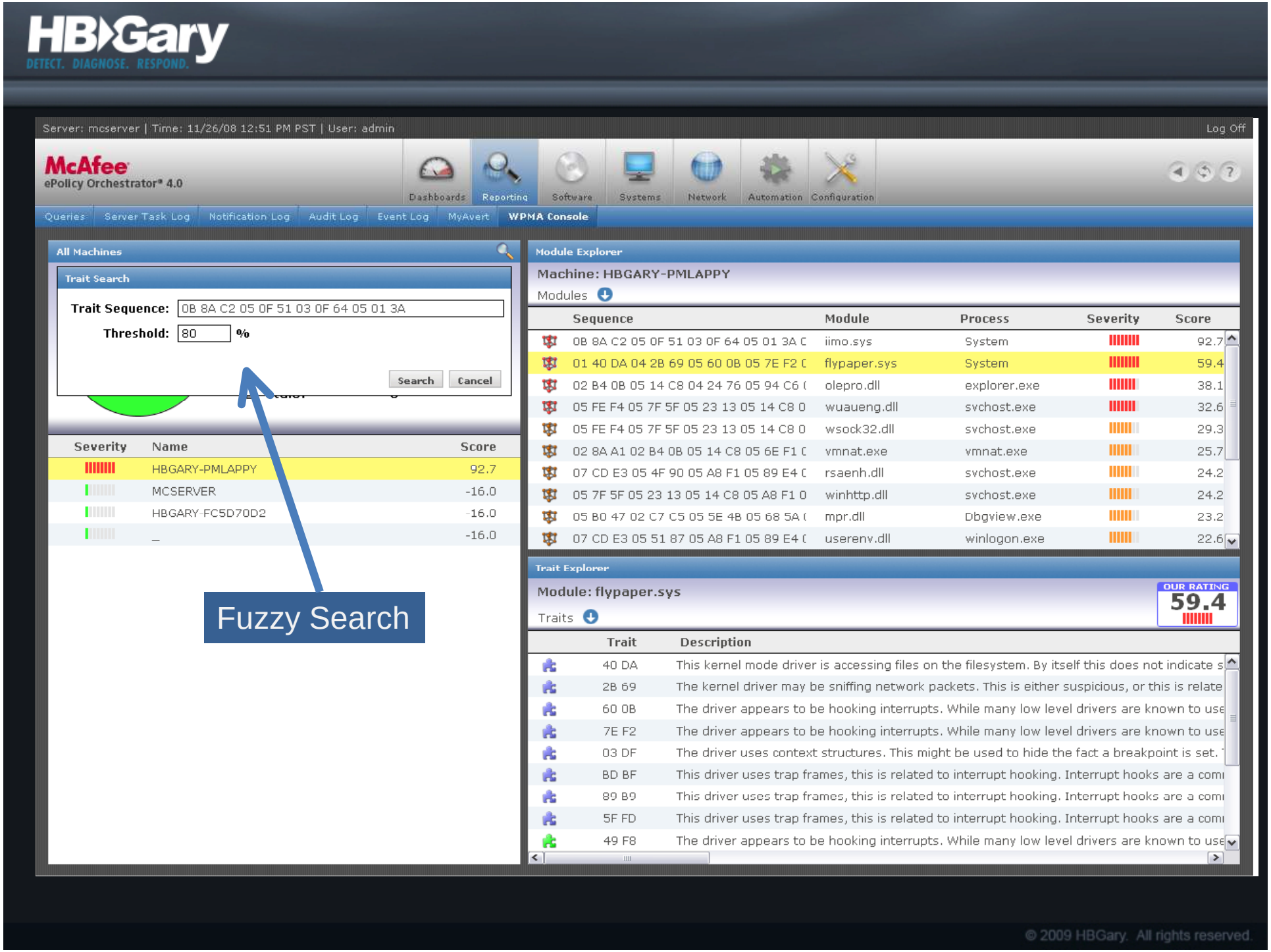
- Digital DNA for McAfee ePO
- Digital DNA for HBGary Active Defense
- Digital DNA for Guidance EnCase Enterprise
- Digital DNA for Verdaysys Digital Guardian

HBGary
DETECT. DIAGNOSE. RESPOND.

Integration with McAfee ePO




HBGary
DETECT. DIAGNOSE. RESPOND.
Server: mcserver | Time: 11/26/08 12:51 PM PST | User: admin
Log Off
McAfee
ePolicy Orchestrator® 4.0
Dashboards
Reporting
Software
Systems
Network
Automation
Configuration
Queries
Server Task Log
Notification Log
Audit Log
Event Log
MyAvert
WPMA Console
All Machines
Total Machines: 4
High Risk: 1
Medium Risk: 0
Low Risk: 0
No Risk: 3
Unscanned: 0
Stale: 0
Severity Name Score
HBGARY-PMLAPPY 92.7
MCSERVER -16.0
HBGARY-FC5D70D2 -16.0
_ -16.0
Module Explorer
Machine: HBGARY-PMLAPPY
Modules
Sequence Module Process Severity Score
0B 8A C2 05 0F 51 03 0F 64 05 01 3A C iimo.sys System 92.7
01 40 DA 04 2B 69 05 60 0B 05 7E F2 C flypaper.sys System 59.4
02 B4 0B 05 14 C8 04 24 76 05 94 C6 (olepro.dll explorer.exe 38.1
05 FE F4 05 7F 5F 05 23 13 05 14 C8 0 wuaueng.dll svchost.exe 32.6
05 FE F4 05 7F 5F 05 23 13 05 14 C8 0 wsock32.dll svchost.exe 29.3
02 8A A1 02 B4 0B 05 14 C8 05 6E F1 C vmnat.exe vmnat.exe 25.7
07 CD E3 05 4F 90 05 A8 F1 05 89 E4 C rsaenh.dll svchost.exe 24.2
05 7F 5F 05 23 13 05 14 C8 05 A8 F1 0 winhttp.dll svchost.exe 24.2
05 B0 47 02 C7 C5 05 5E 4B 05 68 5A (mpr.dll Dbgview.exe 23.2
07 CD E3 05 51 87 05 A8 F1 05 89 E4 C userenv.dll winlogon.exe 22.6
Trait Explorer
Module: flypaper.sys
OUR RATING
59.4
Traits
Trait Description
40 DA This kernel mode driver is accessing files on the filesystem. By itself this does not indicate s
2B 69 The kernel driver may be sniffing network packets. This is either suspicious, or this is relate
60 0B The driver appears to be hooking interrupts. While many low level drivers are known to use
7E F2 The driver appears to be hooking interrupts. While many low level drivers are known to use
03 DF The driver uses context structures. This might be used to hide the fact a breakpoint is set.
BD BF This driver uses trap frames, this is related to interrupt hooking. Interrupt hooks are a comi
89 B9 This driver uses trap frames, this is related to interrupt hooking. Interrupt hooks are a comi
5F FD This driver uses trap frames, this is related to interrupt hooking. Interrupt hooks are a comi
49 F8 The driver appears to be hooking interrupts. While many low level drivers are known to use
© 2009 HBGary. All rights reserved.



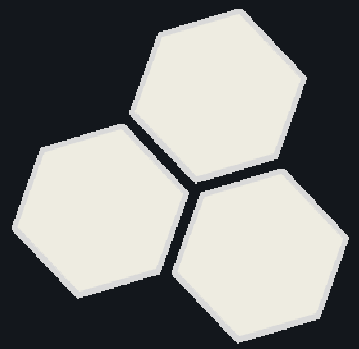
HBGary
DETECT. DIAGNOSE. RESPOND.

Responder

HBGary
DETECT. DIAGNOSE. RESPOND.

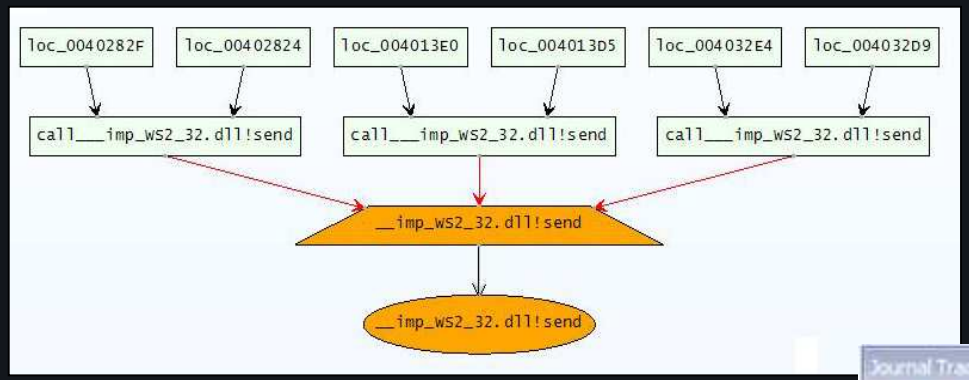
HBGary Responder Professional

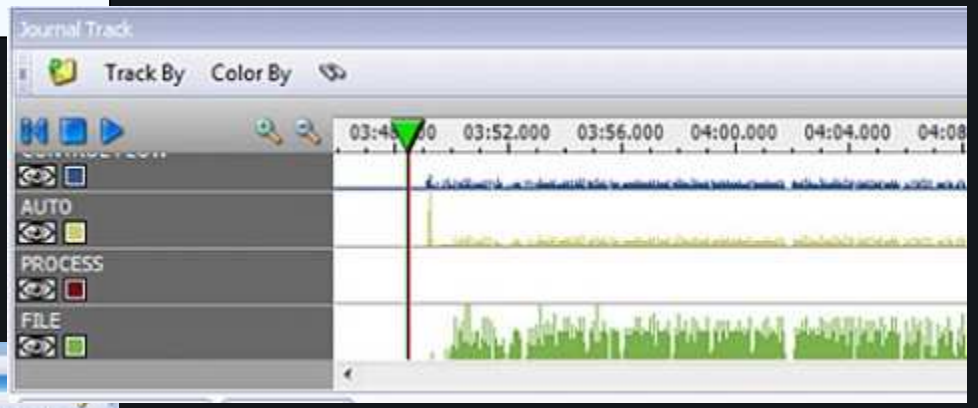
- Standalone system for incident response
- Memory forensics
- Malware reverse engineering
  - Static and dynamic analysis
- Digital DNA module
- REcon module

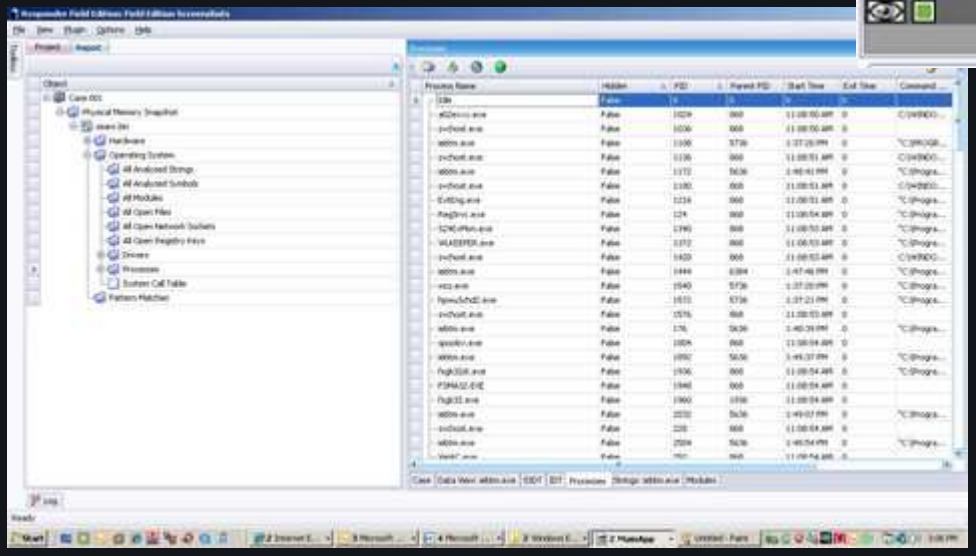


HBGary
DETECT. DIAGNOSE. RESPOND.

Responder Professional







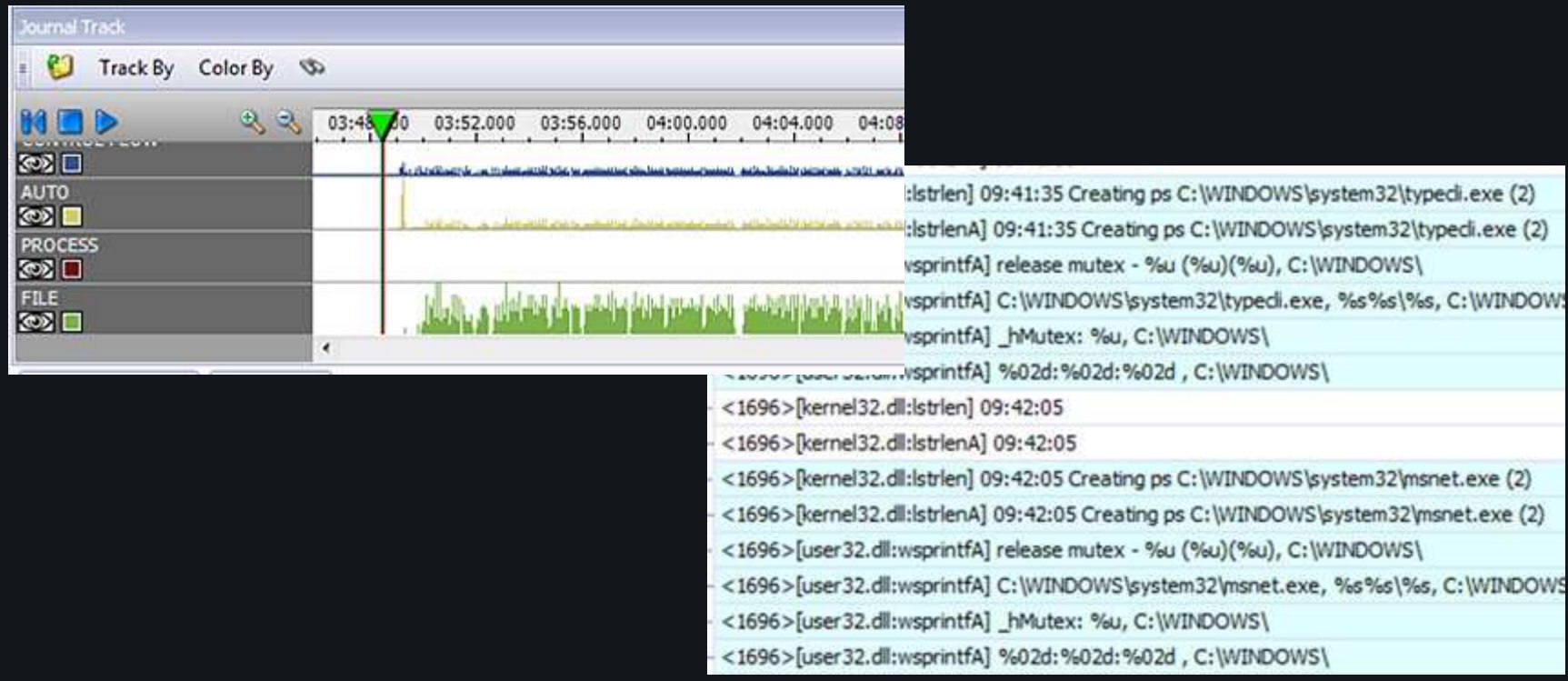
HBGary
DETECT. DIAGNOSE. RESPOND.

REcon

HBGary
DETECT. DIAGNOSE. RESPOND.

REcon

Records the entire lifecycle of a software program, from first instruction to the last.
It records data samples at every step, including arguments to functions and pointers to objects.



HBGary
DETECT. DIAGNOSE. RESPOND.

Advanced Discussion: How HBGary maintains DDNA with Threat Intelligence

HBGary
DETECT. DIAGNOSE. RESPOND.

Intelligence Feed

Partnership Feed Agreements

Feed Processor

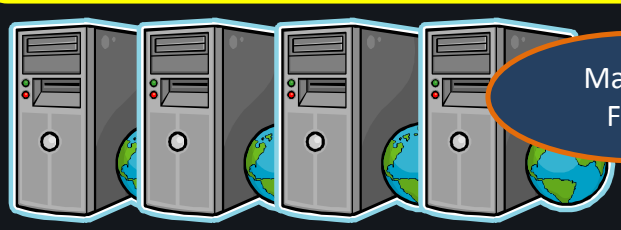
Cyveillance

shadowserver

AV-TEST

McAfee

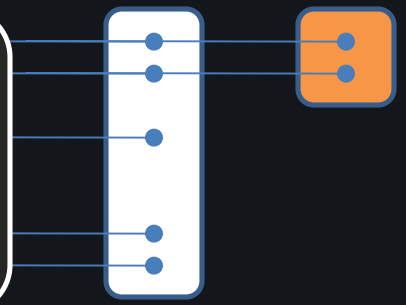
Sources



Machine Farm

Meta Data

Digital DNA



HBGary
DETECT. DIAGNOSE. RESPOND.

From raw data to intelligence

Feed Processor

Meta Data

Digital DNA

Active Defense

primary

Data Integration

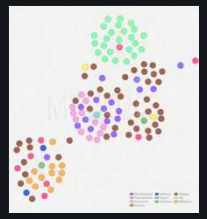
Responder

Malware Analysis

Stalker

Palantir

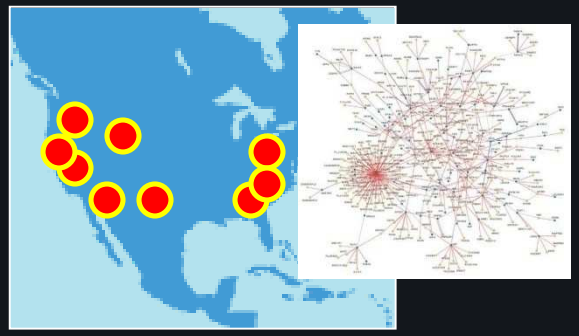
Stats

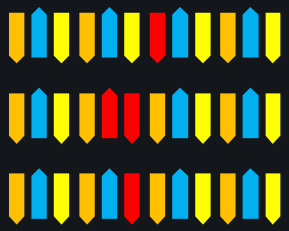


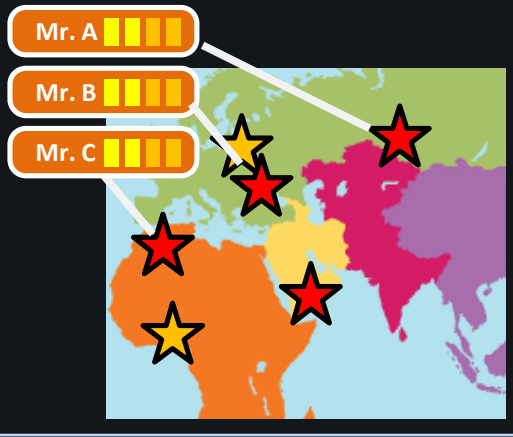
Link Analysis

HBGary
DETECT. DIAGNOSE. RESPOND.

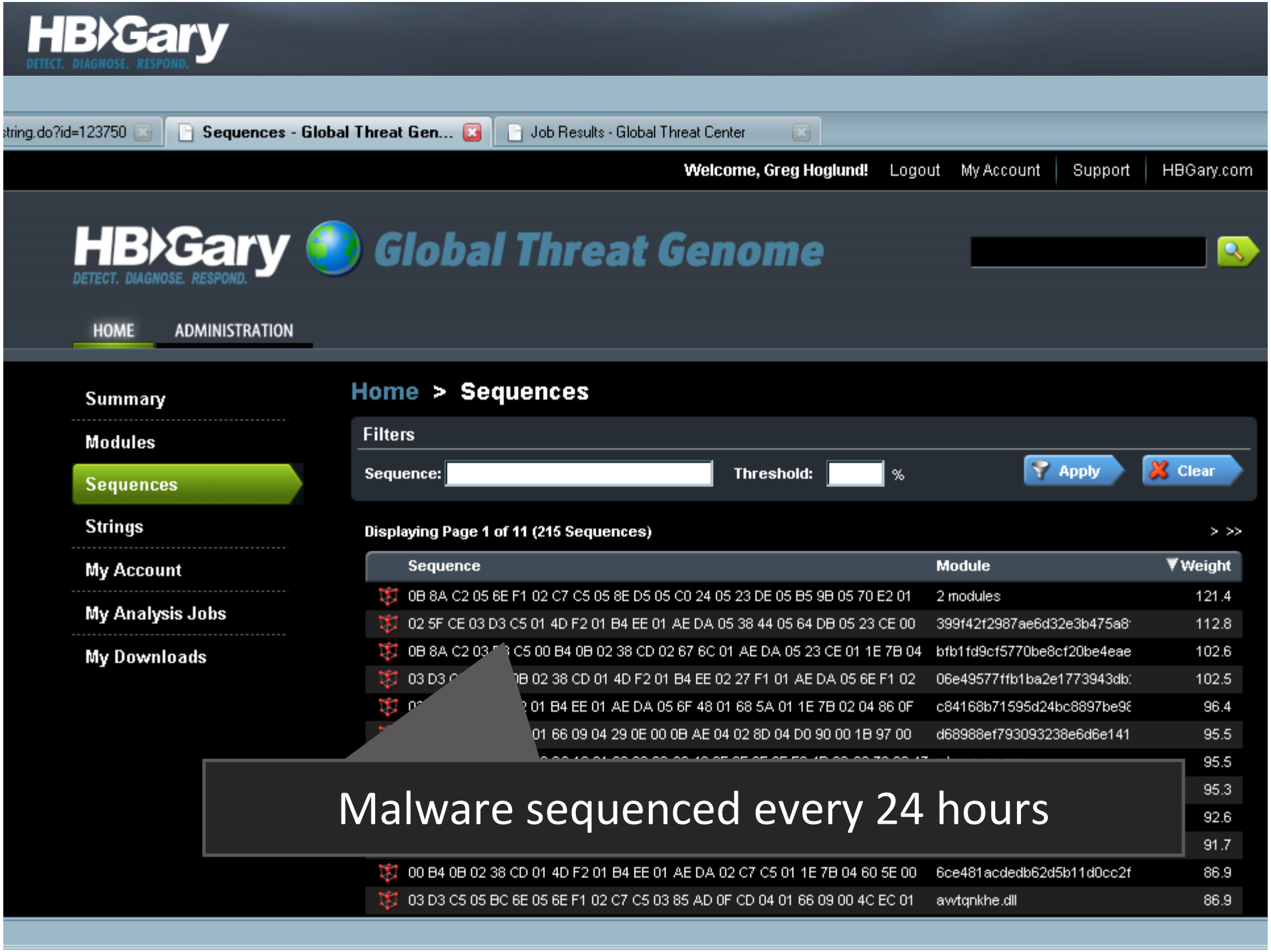
Ops path

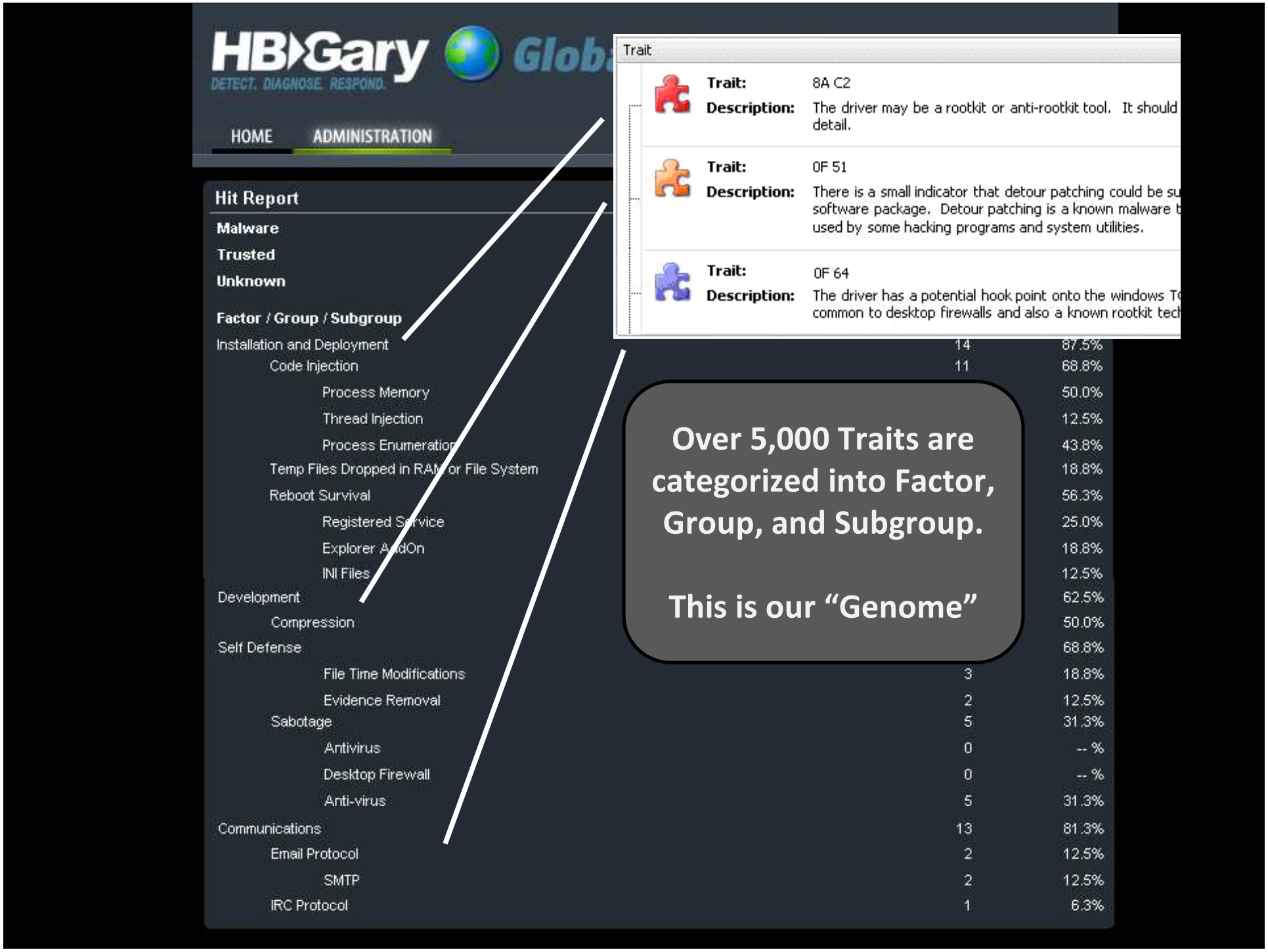






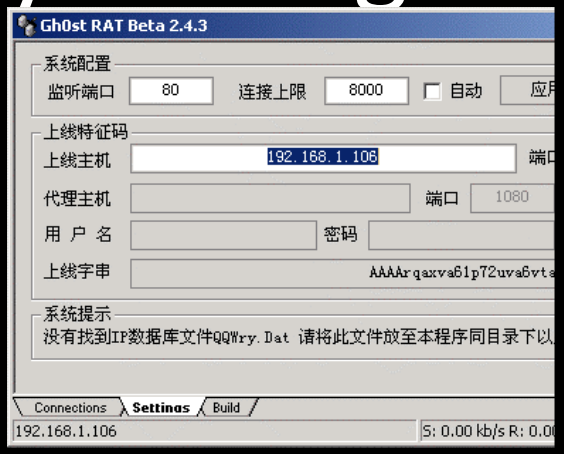
Malware Attack Tracking	Digital DNA™	Active Threat Tracking
Detect relevant attacks in progress. Determine the scope of the attack. Focus is placed on • Botnet / Web / Spam Distribution systems • Potentially targeted spear/whalefishing • Internal network infections at customer sites	Development idioms are fingerprinted. Malware is classified into attribution domains. Special attention is placed on: • Specialized attacks • Targeted attacks • Newly emergent methods	Determine the person(s) operating the attack, and their intent: Leasing Botnet / Spam Financial Fraud Identity Theft Pump and Dump Targeted Threat Email & Documents Theft Intellectual Property Theft Deeper penetration

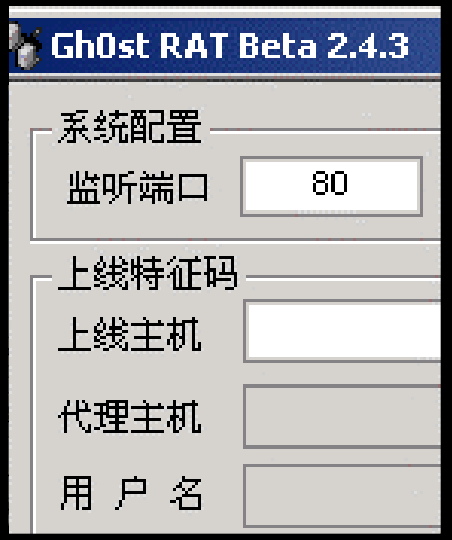

HBGary
DETECT. DIAGNOSE. RESPOND.
tring.do?id=123750
Sequences - Global Threat Gen...
Job Results - Global Threat Center
Welcome, Greg Hoglund!
Logout
My Account
Support
HBGary.com
HBGary
DETECT. DIAGNOSE. RESPOND.
Global Threat Genome
HOME
ADMINISTRATION
Summary
Modules
Sequences
Strings
My Account
My Analysis Jobs
My Downloads
Home > Sequences
Filters
Sequence:
Threshold:
%
Apply
Clear
Displaying Page 1 of 11 (215 Sequences)
> >>
Sequence
Module
Weight
0B 8A C2 05 6E F1 02 C7 C5 05 8E D5 05 C0 24 05 23 DE 05 B5 9B 05 70 E2 01
2 modules
121.4
02 5F CE 03 D3 C5 01 4D F2 01 B4 EE 01 AE DA 05 38 44 05 64 DB 05 23 CE 00
399f42f2987ae6d32e3b475a8
112.8
0B 8A C2 03
C5 00 B4 0B 02 38 CD 02 67 6C 01 AE DA 05 23 CE 01 1E 7B 04
bfb1fd9cf5770be8cf20be4eae
102.6
03 D3
0B 02 38 CD 01 4D F2 01 B4 EE 02 27 F1 01 AE DA 05 6E F1 02
06e49577ffb1ba2e1773943db
102.5
01 B4 EE 01 AE DA 05 6F 48 01 68 5A 01 1E 7B 02 04 86 0F
c84168b71595d24bc8897be9
96.4
01 66 09 04 29 0E 00 0B AE 04 02 8D 04 D0 90 00 1B 97 00
d68988ef793093238e6d6e141
95.5
95.5
95.3
92.6
91.7
00 B4 0B 02 38 CD 01 4D F2 01 B4 EE 01 AE DA 02 C7 C5 01 1E 7B 04 60 5E 00
6ce481acdedb62d5b11d0cc2f
86.9
03 D3 C5 05 BC 6E 05 6E F1 02 C7 C5 03 85 AD 0F CD 04 01 66 09 00 4C EC 01
awtqnkhe.dll
86.9
Malware sequenced every 24 hours

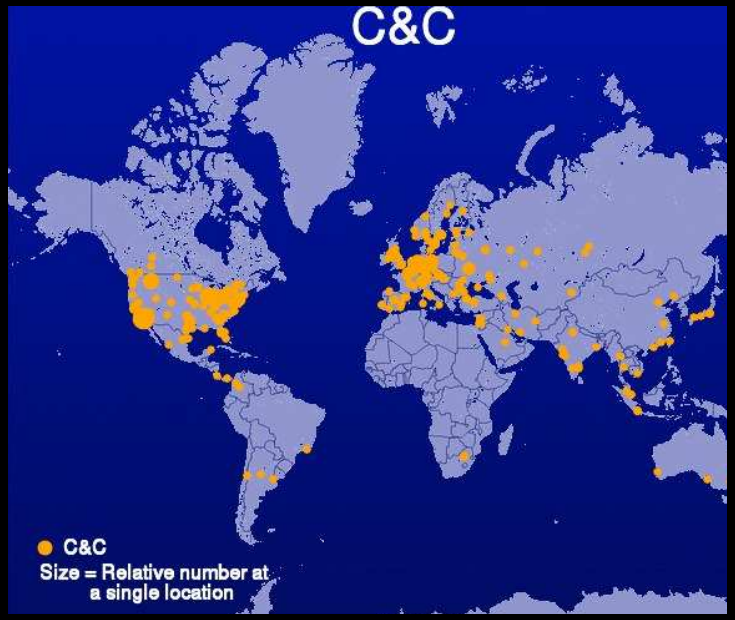

HBGary
DETECT. DIAGNOSE. RESPOND.
HOME
ADMINISTRATION
Hit Report
Malware
Trusted
Unknown
Factor / Group / Subgroup
Installation and Deployment
Code Injection
Process Memory
Thread Injection
Process Enumeration
Temp Files Dropped in RAM or File System
Reboot Survival
Registered Service
Explorer AddOn
INI Files
Development
Compression
Self Defense
File Time Modifications
Evidence Removal
Sabotage
Antivirus
Desktop Firewall
Anti-virus
Communications
Email Protocol
SMTP
IRC Protocol
14 87.5%
11 68.8%
50.0%
12.5%
43.8%
18.8%
56.3%
25.0%
18.8%
12.5%
62.5%
50.0%
68.8%
3 18.8%
2 12.5%
5 31.3%
0 -- %
0 -- %
5 31.3%
13 81.3%
2 12.5%
2 12.5%
1 6.3%
Trait
Trait: 8A C2
Description: The driver may be a rootkit or anti-rootkit tool. It should
detail.
Trait: 0F 51
Description: There is a small indicator that detour patching could be su
software package. Detour patching is a known malware t
used by some hacking programs and system utilities.
Trait: 0F 64
Description: The driver has a potential hook point onto the windows T
common to desktop firewalls and also a known rootkit tech
Over 5,000 Traits are categorized into Factor, Group, and Subgroup.
This is our “Genome”

Country of Origin

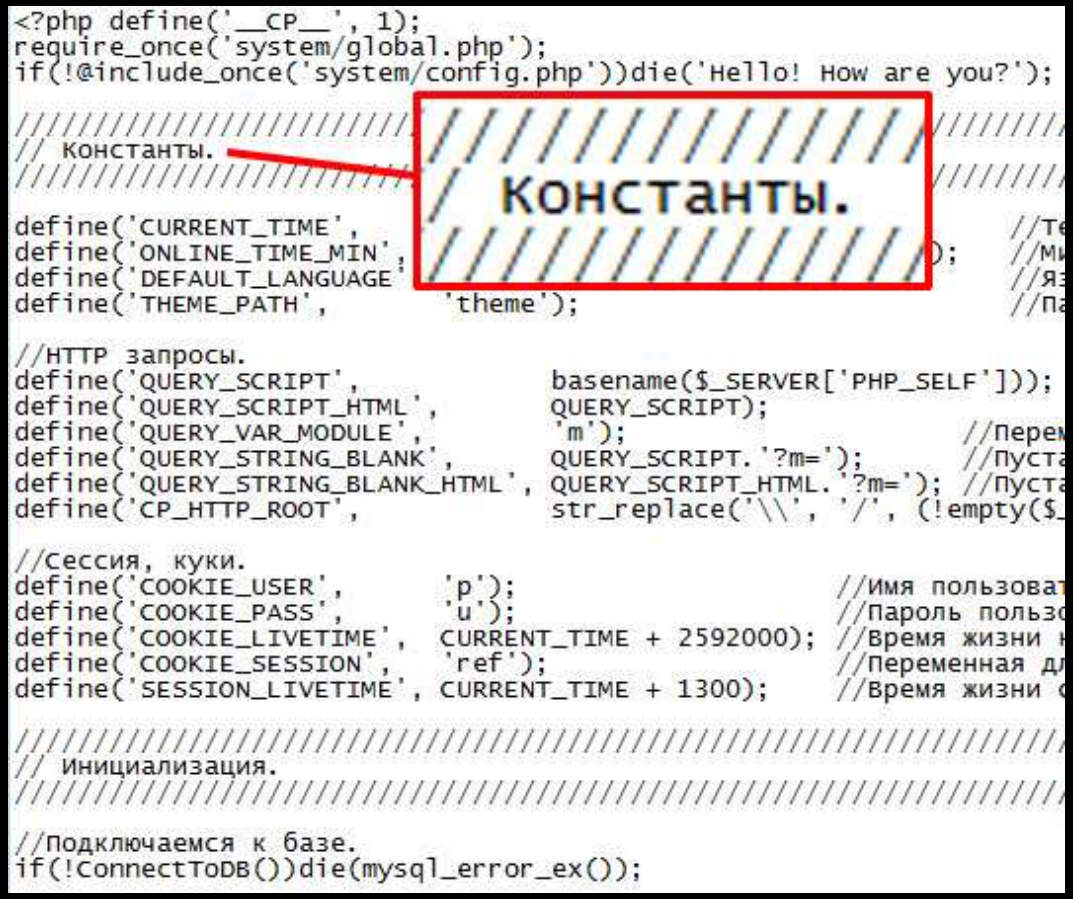
- Country of origin
  - Is the bot designed for use by certain nationality?
- Geolocation of IP is NOT a strong indicator
  - However, there are notable examples
  - Is the IP in a network that is very unlikely to have a third-party proxy installed?
    - For example, it lies within a government installation







C&C map from Shadowserver, C&C for 24 hour period

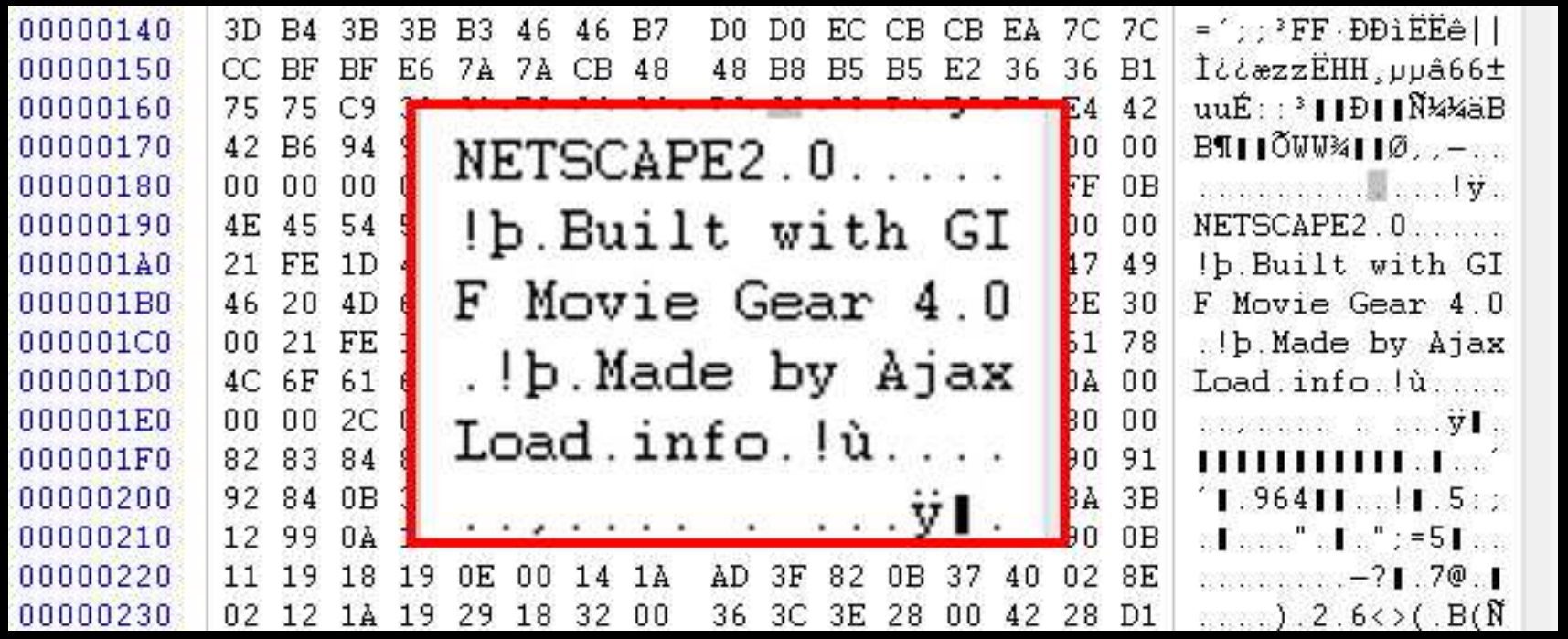



```
<?php define('__CP__', 1);
require_once('system/global.php');
if(!@include_once('system/config.php'))die('Hello! How are you?');

////////////////////////////
// Константы.
////////////////////////////

define('CURRENT_TIME',
define('ONLINE_TIME_MIN',
define('DEFAULT_LANGUAGE'
define('THEME_PATH',        'theme');

//HTTP запросы.
define('QUERY_SCRIPT',             basename($_SERVER['PHP_SELF']));
define('QUERY_SCRIPT_HTML',        QUERY_SCRIPT);
define('QUERY_VAR_MODULE',         'm');
define('QUERY_STRING_BLANK',       QUERY_SCRIPT.'?m=');
define('QUERY_STRING_BLANK_HTML', QUERY_SCRIPT_HTML.'?m=');
define('CP_HTTP_ROOT',             str_replace('\\', '/', (!empty($_

//Сессия, куки.
define('COOKIE_USER',       'p');
define('COOKIE_PASS',       'u');
define('COOKIE_LIVETIME',   CURRENT_TIME + 2592000);
define('COOKIE_SESSION',    'ref');
define('SESSION_LIVETIME', CURRENT_TIME + 1300);

////////////////////////////////////////////////////////////////////
// Инициализация.
////////////////////////////////////////////////////////////////////

//Подключаемся к базе.
if(!ConnectToDB())die(mysql_error_ex());
```

C&C server source code.

1)Written in PHP
2)Specific “Hello” response (note, can be queried from remote to fingerprint server)
3)Clearly written in Russian

In many cases, the authors make no attempt to hide….
You can purchase many kits and just read the source code…



A GIF file included in a C&C server package.

GhostNet: Screen Capture Algorithm

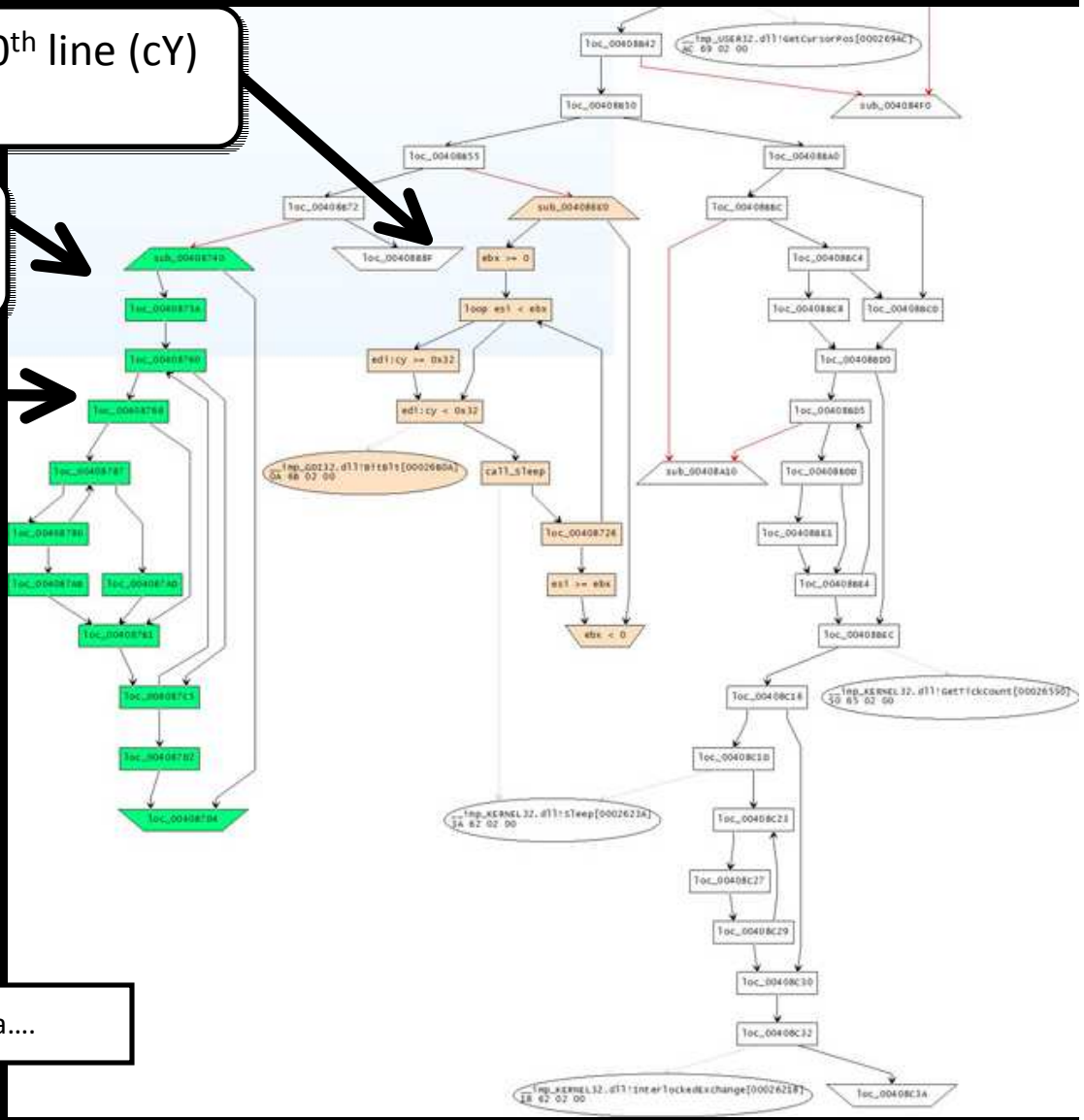
Loops, scanning every 50th line (cY) of the display.

Reads screenshot data, creates a special DIFF buffer

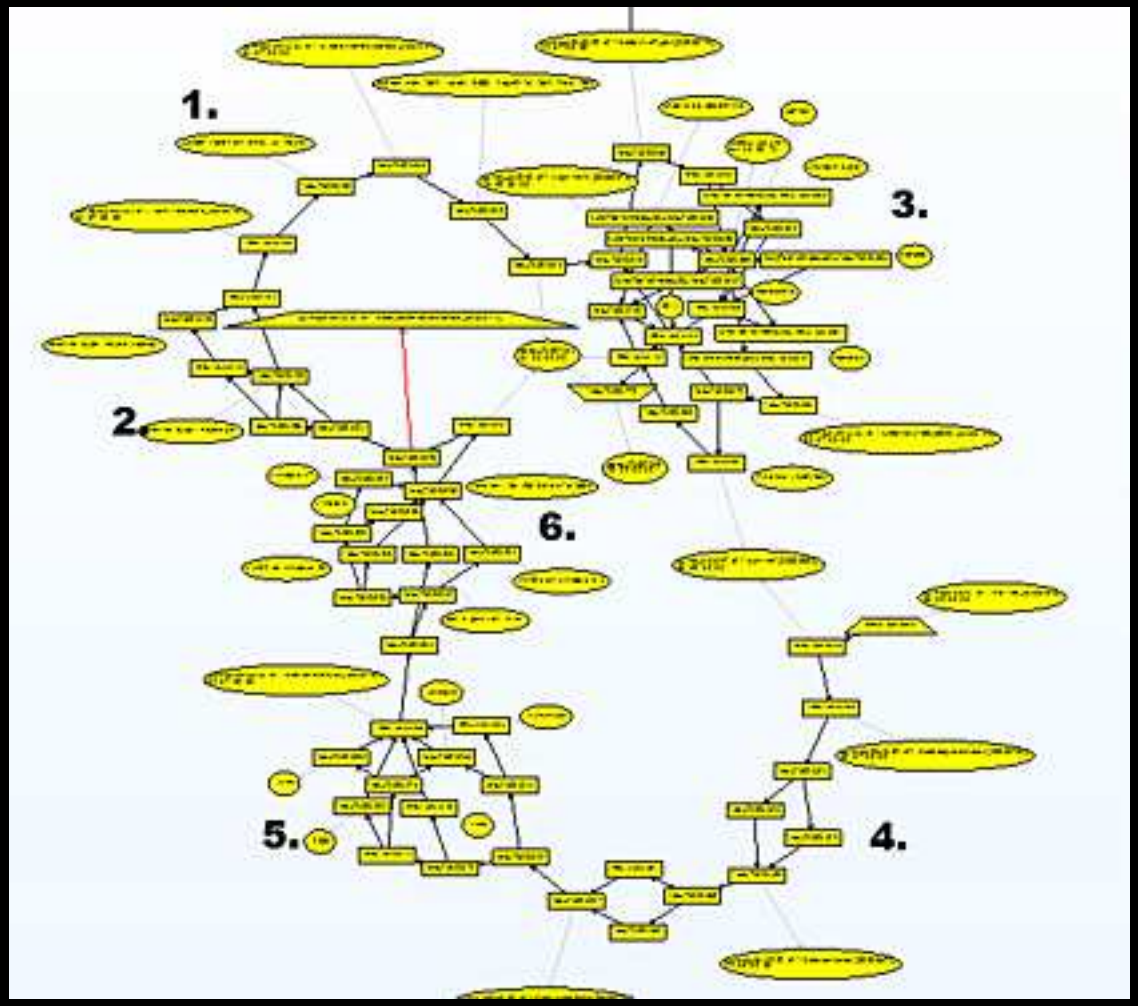
LOOP: Compare new screenshot to previous, 4 bytes at a time

If they differ, enter secondary loop here, writing a ‘data run’ for as long as there is no match.

Offset in screenshot	Len in bytes	Data….

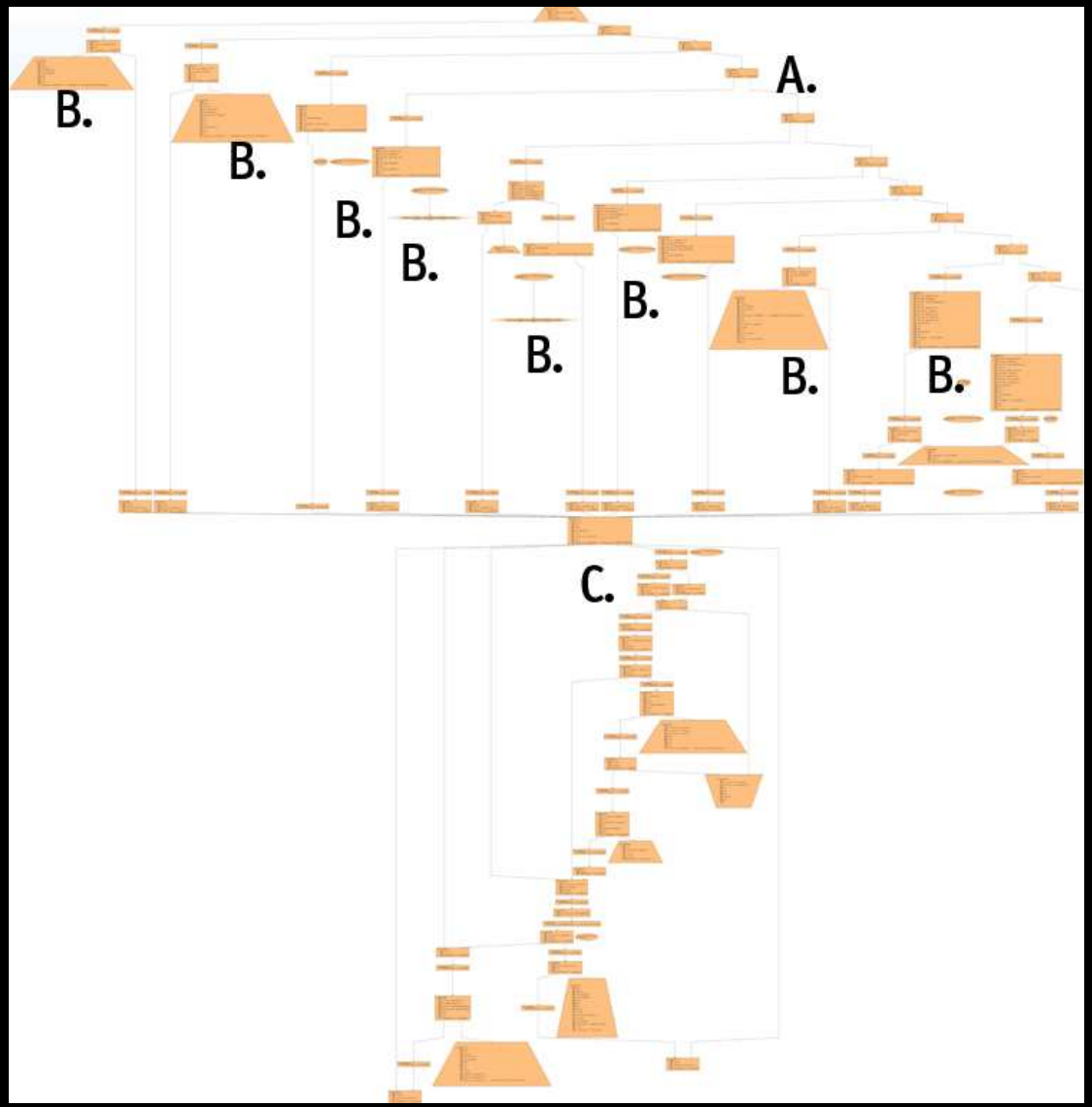


‘Soysauce’ C&C Hello Message



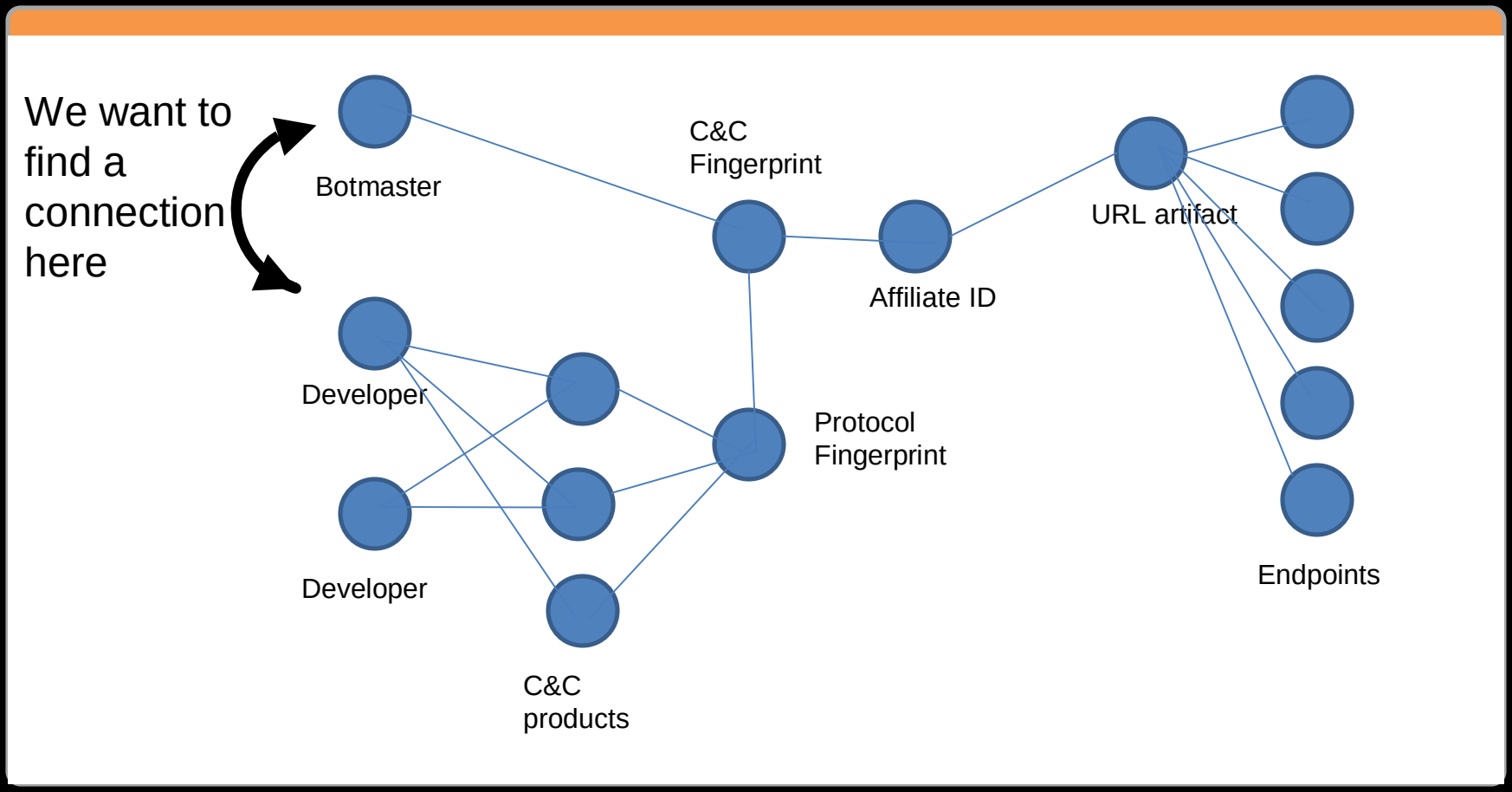
1) this queries the uptime of the machine..
2) checks whether it's a laptop or desktop machine...
3) enumerates all the drives attached to the system, including USB and network...
4) gets the windows username and computername...
5) gets the CPU info... and finally,
6) the version and build number of windows.

Aurora C&C parser



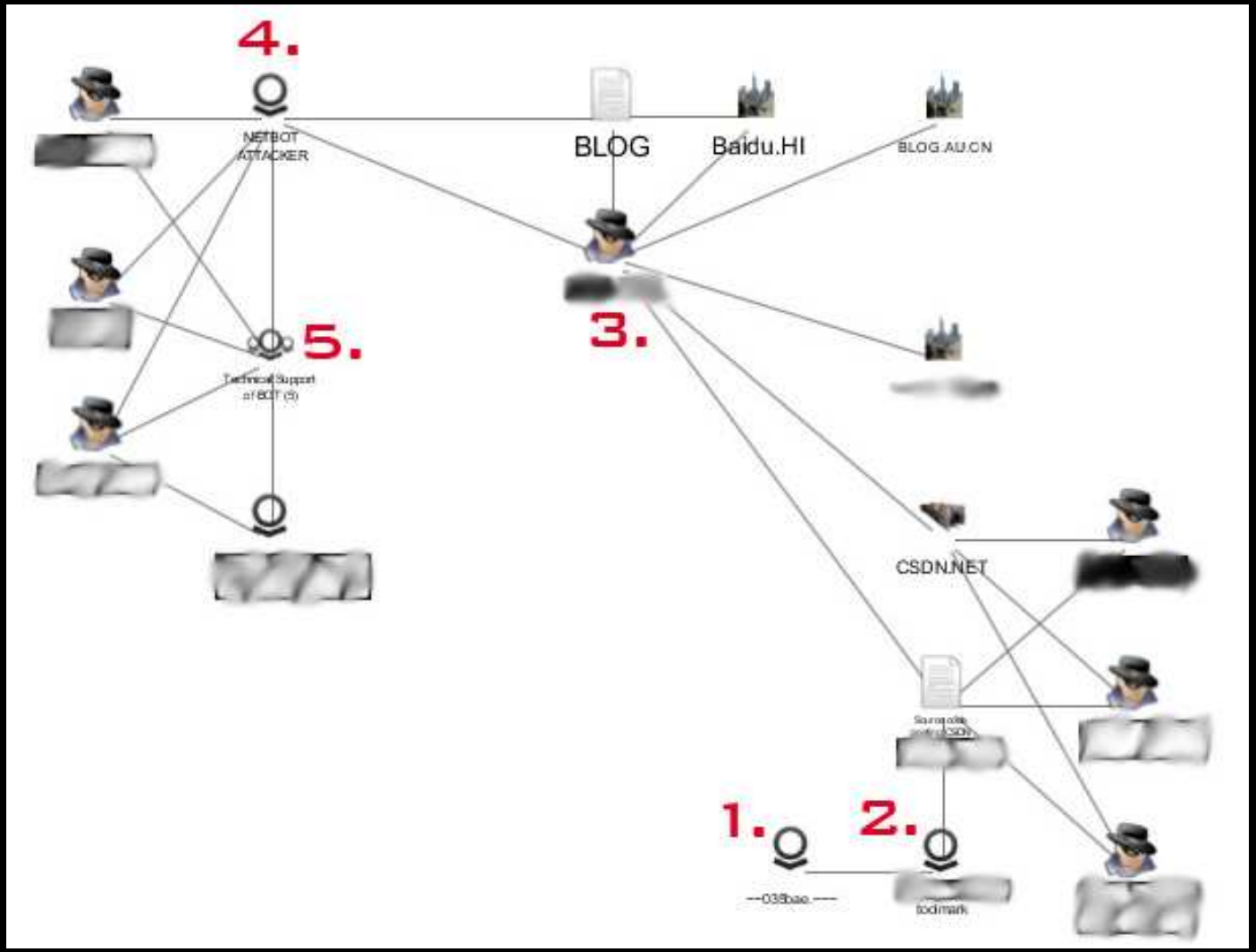
A) Command is stored as a number, not text. It is checked here.
B) Each individual command handler is clearly visible below the numerical check
C) After the command handler processes the command, the result is sent back to the C&C server

Link Analysis



Link Analysis

Example: Link Analysis with Palantir™



1. Implant
2. Forensic Toolmark specific to Implant
3. Searching the ‘Net reveals source code that leads to Actor
4. Actor is supplying a backdoor
5. Group of people asking for technical support on their copies of the backdoor

HBGary
DETECT. DIAGNOSE. RESPOND.

Questions?