HBGary
DEFEATING TOMORROW'S THREAT TODAY

Management Presentation

Prepared for

McAfee®

November 2010, Proprietary and Confidential

© 2009 HBGary. All rights reserved.

HBGary

DETECT. DIAGNOSE. RESPOND.

Continuous Protection

History of Industry Leadership

- Founded in 2003 to perform offensive cyber security consulting for the CIA and other high profile government agencies
- Shifted focus from government consulting which is not scalable to developing security software products
- Offices in Sacramento, and DC Area
- Now serve critical infrastructure customers, with the most sophisticated security demands, across the government and private sectors

© 2009 HBGary. All rights reserved.

HBGary
DETECT. DIAGNOSE. RESPOND.

HBGary Management – Deep Domain Knowledge

Greg Hoglund
CEO

Previous Innovations:
• Wrote early network vulnerability scanners, installed in over half of Fortune 500 companies
•Created and documented the first Windows NT-based rootkit

History of Entrepreneurship:
• Founded www.rootkit.com
• Co-founded Cenzic, Inc., an innovator in software fault injection technology

Publications:
• Exploiting Online Games (Addison Wesley 2007)
•Rootkits: Subverting the Windows Kernal (Addison Wesley 2005)
•Exploiting Software: How to Break Code (Addison Wesley 2004)

Additional:
• Holds two patents
• Frequent speaker at Black Hat, RSA and other security conferences

Penny Leavy
President

Previous Experience:
• Co-founded Cenzic:
  • Formulated Cenzic's basic business structure
  • Assembled a solid executive team
  • Secured financing from top-tier venture capital firms during a tight economy

•Head of sales for FTP Software:
  • Built a distribution network of over 500 OEM and channel partners
  • Opened nine international sales offices
  • Grew sales from $3 million to $120 million

- Finjan Software:
  - Instrumental in repositioning the Company as a leading corporate-security provider

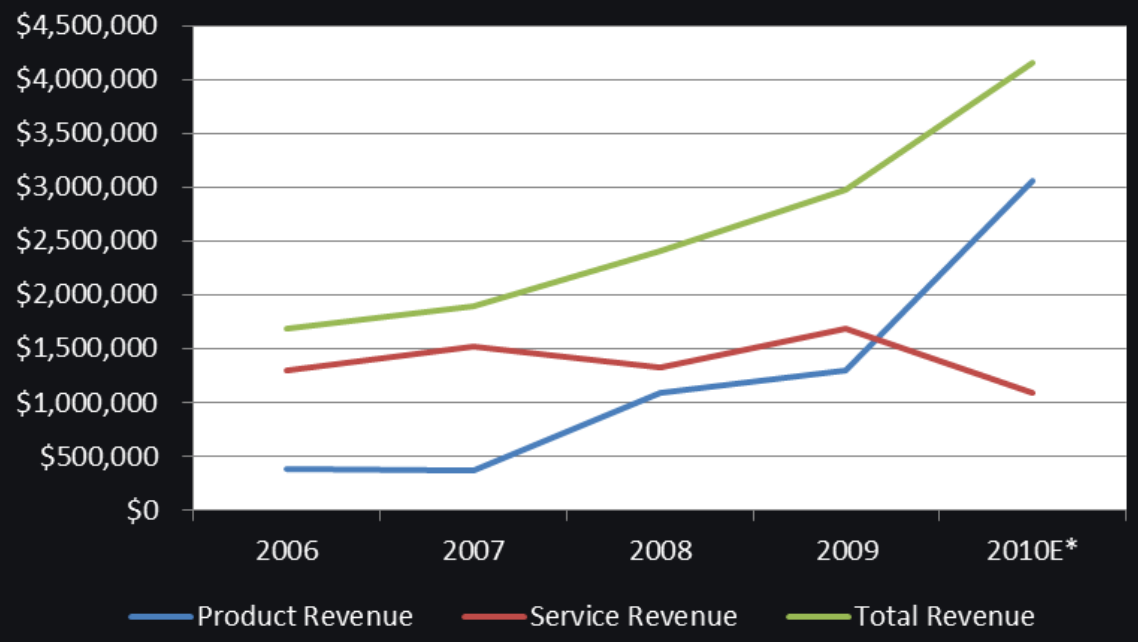
- Tripwire:
  - Developed an aggressive product strategy that resulted in increased visibility and revenues for the computer security company

© 2009 HBGary. All rights reserved.

High-Value Partnerships Drive Strong Growth in Sales

© 2009 HBGary. All rights reserved.

History of Solid Revenue Growth



HBGary has experienced tremendous revenue growth since 2006, driven primarily by the strong growth in product revenue:

CAGR	
Product Revenue	67%
Service Revenue	-4%
Total Revenue	25%

© 2009 HBGary. All rights reserved.

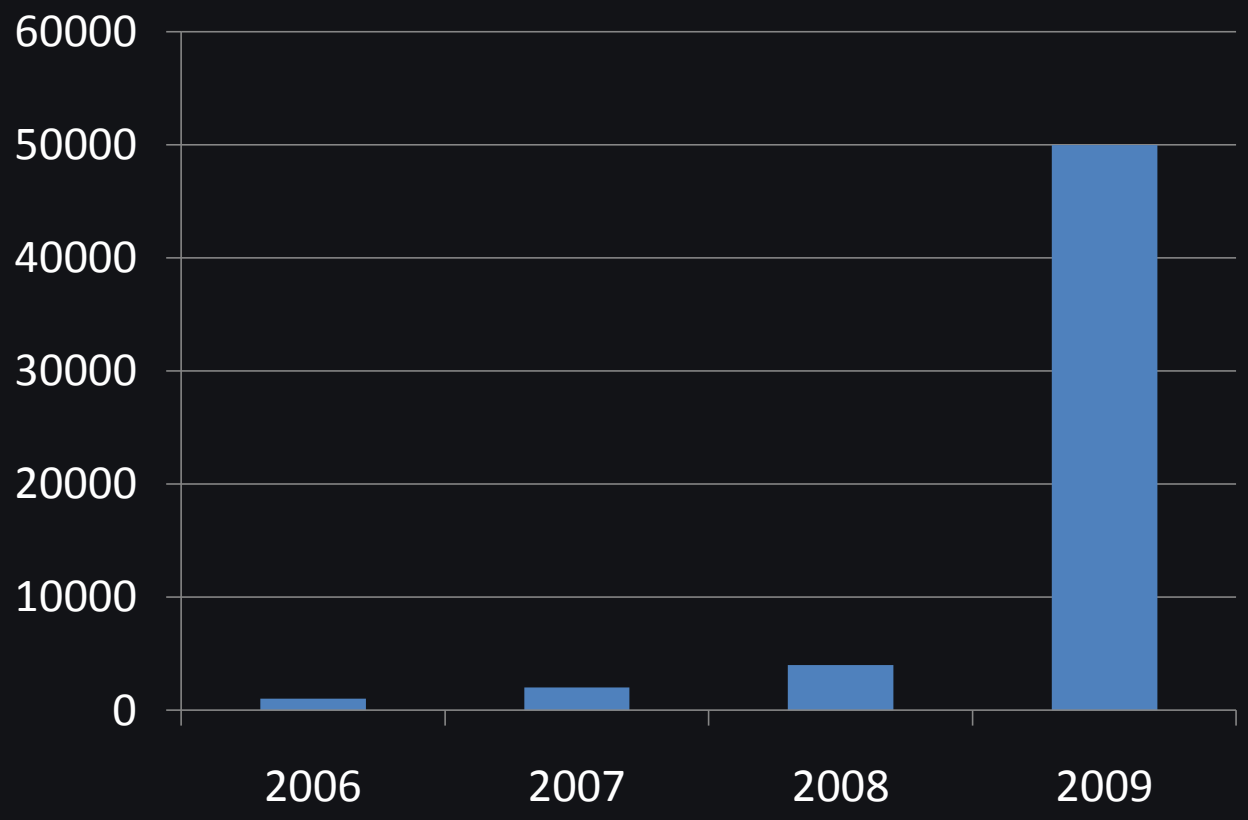
The Evolved Risk Environment

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 and perimeter protection is incomplete. Existing security does not detect emerging threats. The network is becoming perimeterless and the host is the key to protecting the enterprise

© 2009 HBGary. All rights reserved.

Signature based systems don't scale



© 2009 HBGary. All rights reserved.

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*)

© 2009 HBGary. All rights reserved.

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.

© 2009 HBGary. All rights reserved.

Efficient & Scalable Visibility

- To detect advanced intruders, the security 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

© 2009 HBGary. All rights reserved.

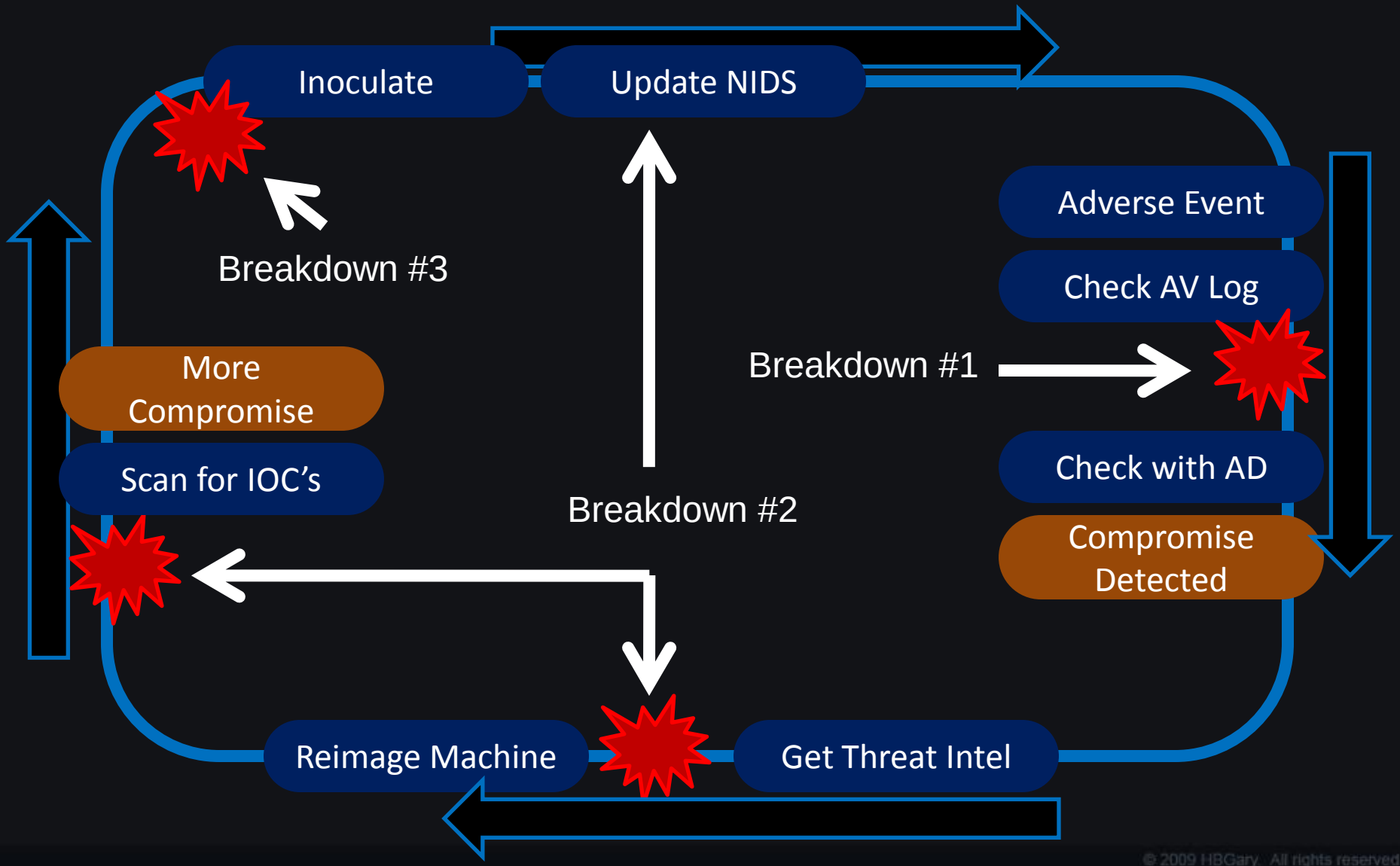
Countermeasures

- 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.

© 2009 HBGary. All rights reserved.

HBGary
DETECT. DIAGNOSE. RESPOND.

Continuous Protection



© 2009 HBGary. All rights reserved.

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

© 2009 HBGary. All rights reserved.

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
- Inoculate to protect against known malware
- Back this with very low level & sophisticated deep-dive capability for attribution and forensics work=Smarter Security

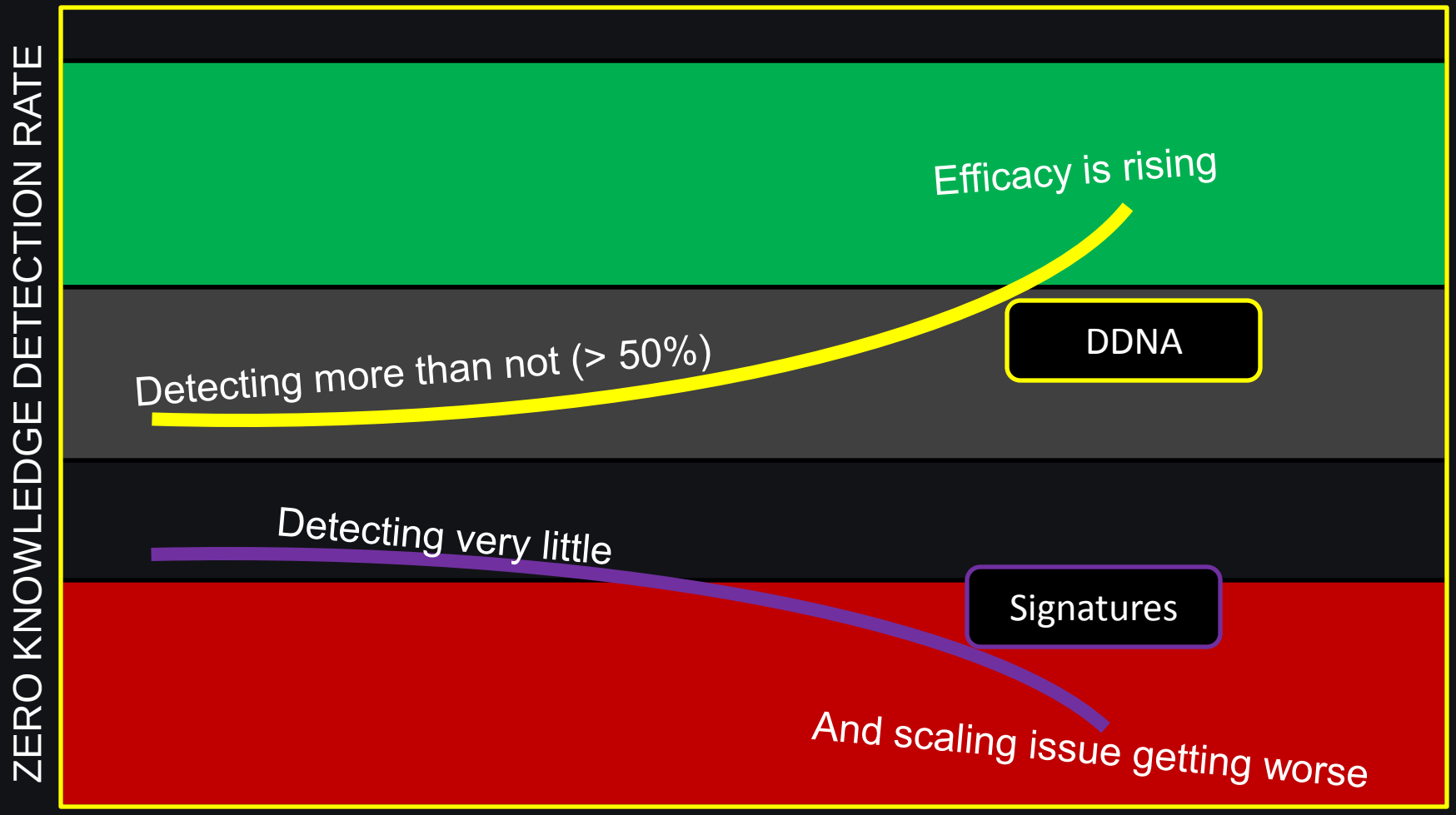
© 2009 HBGary. All rights reserved.

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

© 2009 HBGary. All rights reserved.

Efficacy Curve



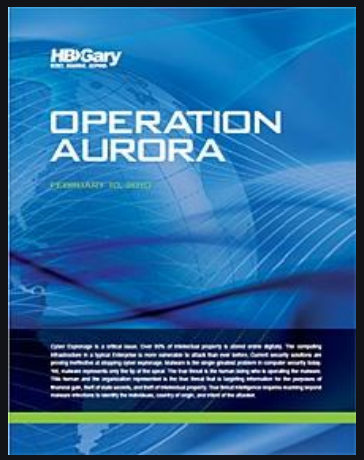
© 2009 HBGary. All rights reserved.

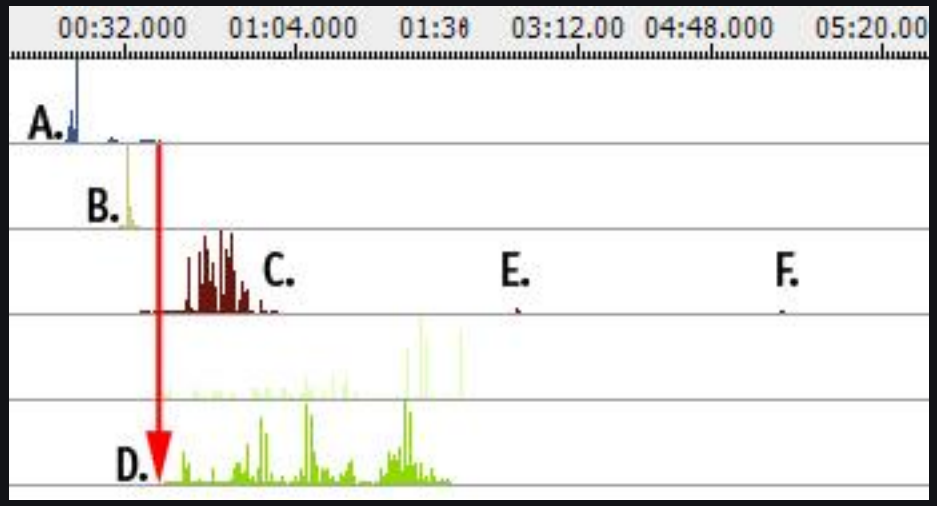
And The Very Near Future

- 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

© 2009 HBGary. All rights reserved.

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
```

© 2009 HBGary. All rights reserved.

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

© 2009 HBGary. All rights reserved.

High Profile Customers

Government Agencies:
Department of Homeland Security
National Security Agency Blue Team
92nd Airborne
Federal Bureau of Investigation
Congressional Budget Office
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

Fortune 500 Corporations:
Morgan Stanley
Sony
Citigroup
IBM
General Electric
Cox Cable
eBay
JP Morgan
Best Buy
Pfizer
Baker Hughes
Fidelity

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

© 2009 HBGary. All rights reserved.

HBGary
DETECT. DIAGNOSE. RESPOND.

HBGary Customers: 100% Referencable

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

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

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

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."

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."

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

© 2009 HBGary. All rights reserved.

HBGary
DETECT. DIAGNOSE. RESPOND.

Managed Service

Managed Service

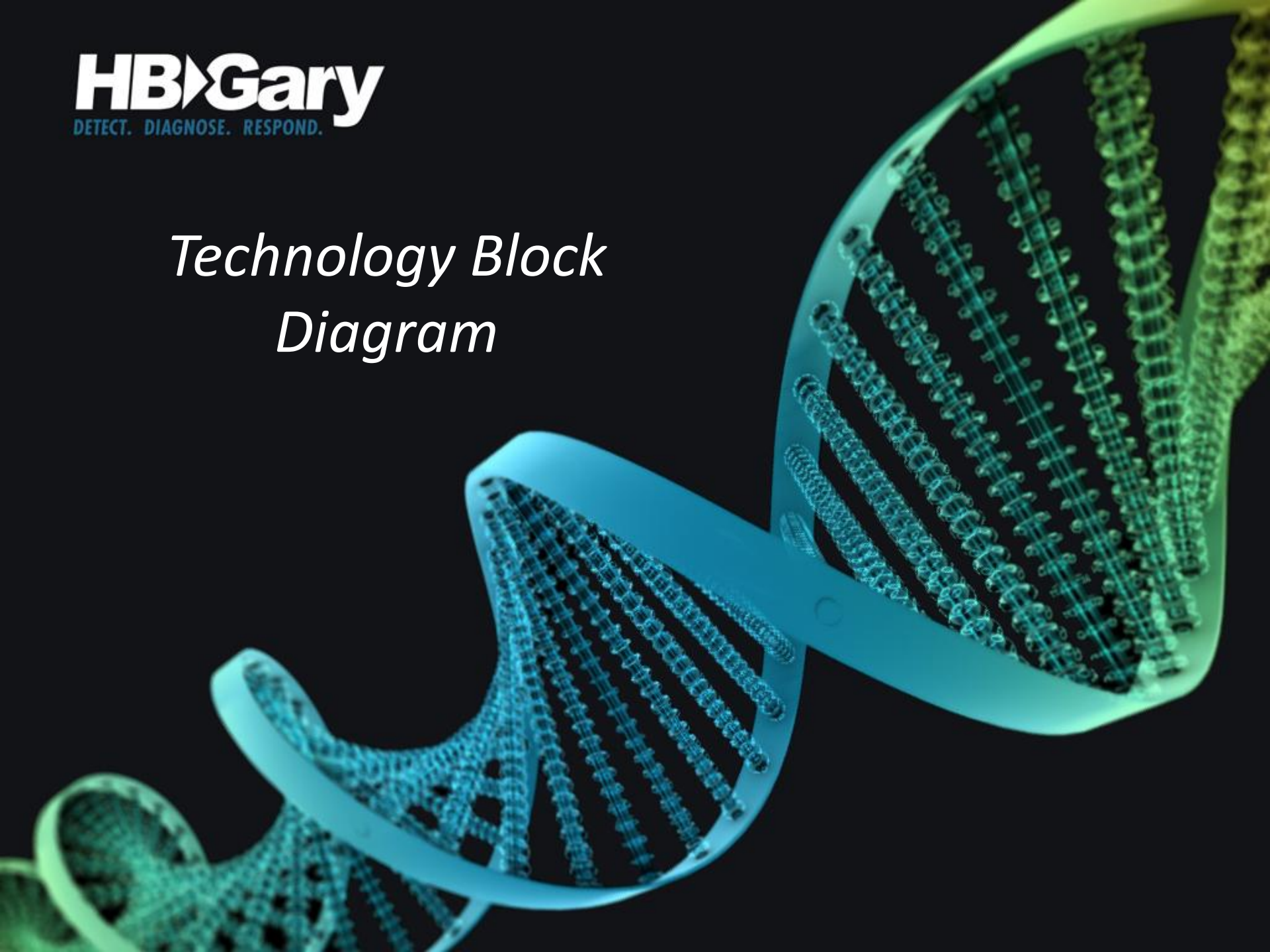
- Weekly, enterprise-wide scanning with DDNA & updated IOC's (using HBGary Product)
- Includes extraction of threat-intelligence from compromised systems and malware
- Includes creation of new IDS signatures
- Includes inoculation shot development
- Includes option for network monitoring specifically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

© 2009 HBGary. All rights reserved.

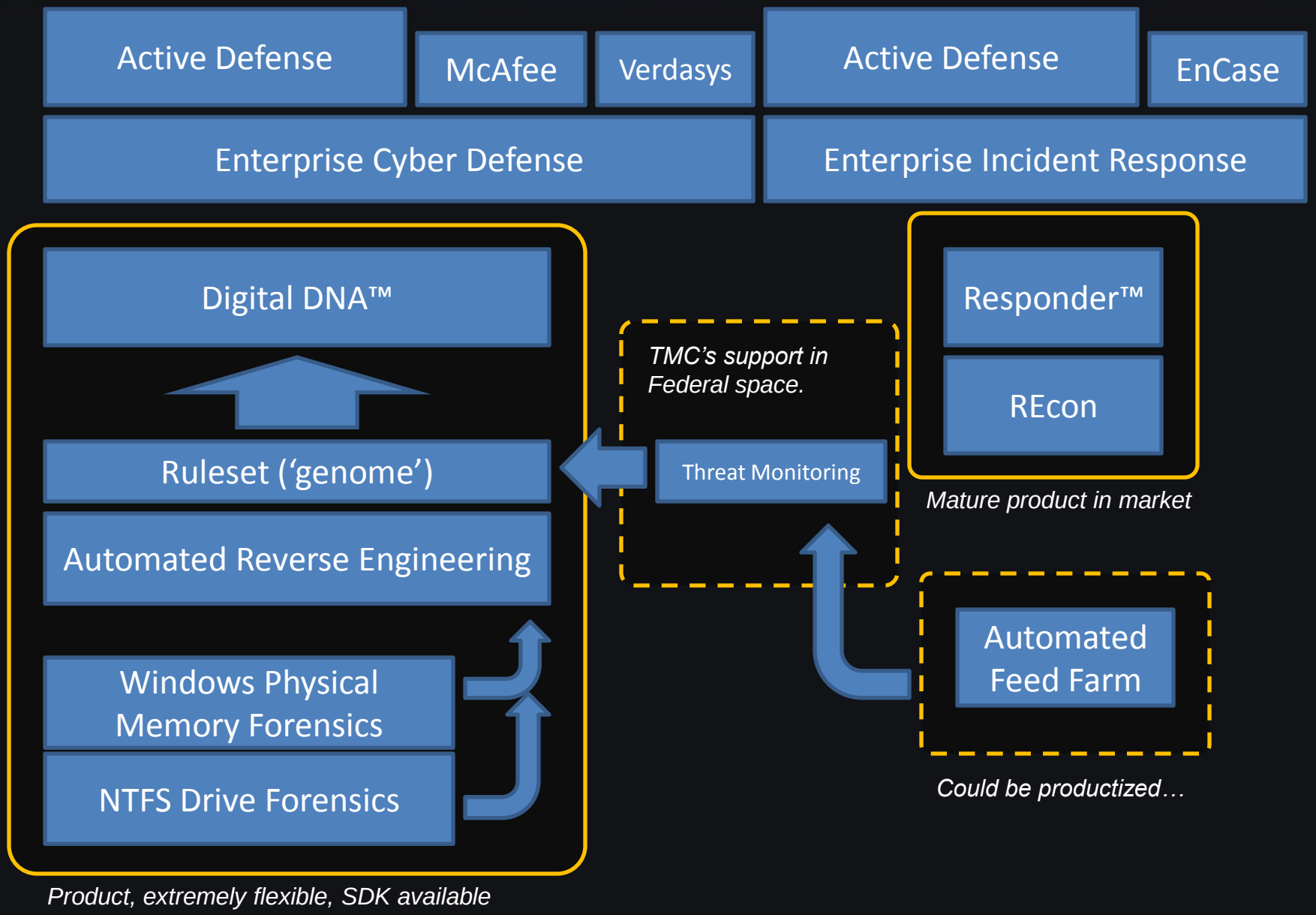
HBGary

DETECT. DIAGNOSE. RESPOND.

Technology Block Diagram



HBGary
DETECT. DIAGNOSE. RESPOND.



© 2009 HBGary. All rights reserved.

HBGary
DETECT. DIAGNOSE. RESPOND.

Digital DNA™

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

© 2009 HBGary. All rights reserved.

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

© 2009 HBGary. All rights reserved.

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

© 2009 HBGary. All rights reserved.

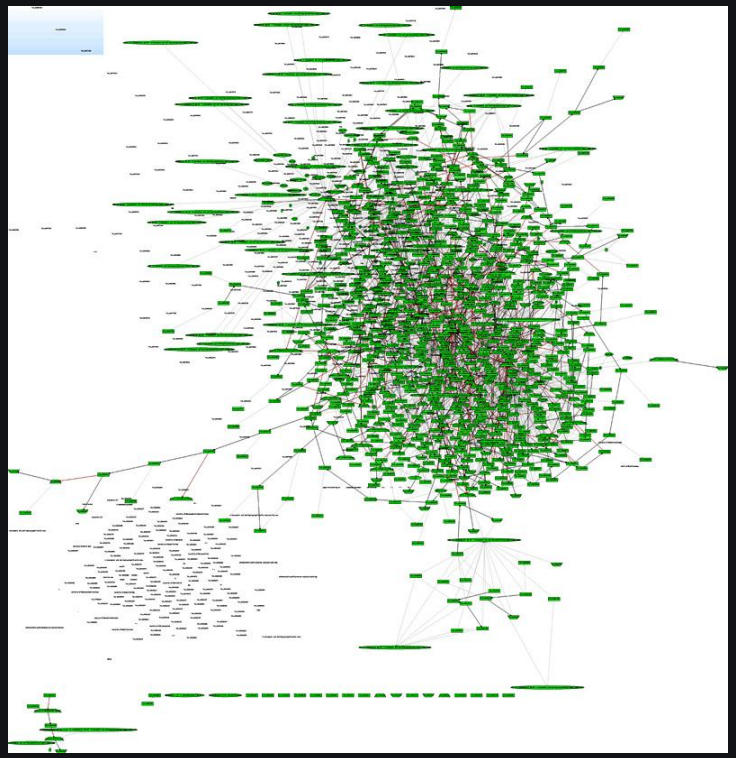
Digital DNA™ Performance

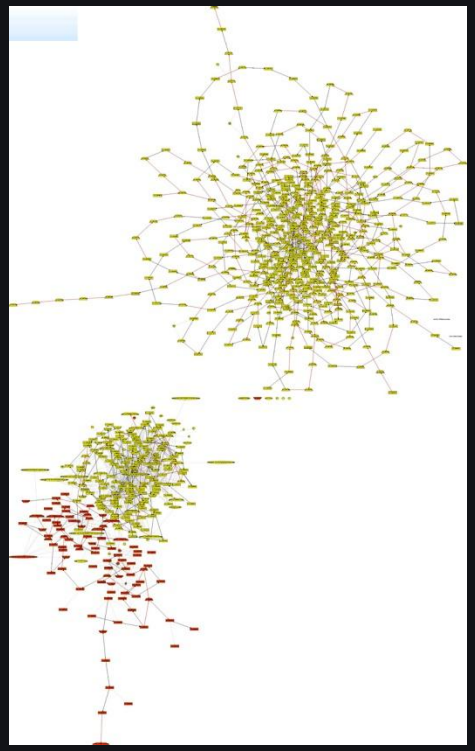
- 4 gigs per minute, thousands of patterns in parallel, NTFS raw disk, end node
- 2 gig memory, 5 minute scan, end node
- Hi/Med/Low throttle
- = 10,000 machine scan completes in < 1 hour

© 2009 HBGary. All rights reserved.

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.





© 2009 HBGary. All rights reserved.

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 8A ... 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

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.

Software Behavioral Traits

© 2009 HBGary. All rights reserved.

What's in a Trait?

04 0F 51

```
B[00 24 73 ??]k ANDS[>004]
C"QueueAPC"{arg0:0A,arg}
```

The rule is a specified like a regular expression, it matches against automatically reverse engineered details and contains boolean logic. These rules are considered intellectual property and not shown to the user.

Unique hash code

Weight / Control flags

The trait, description, and underlying rule are held in a database

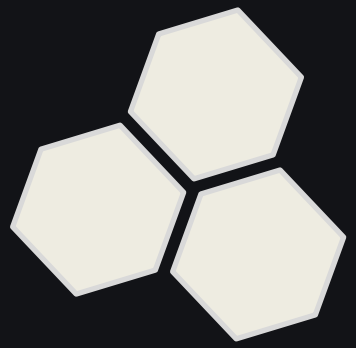
Trait: 0F 51

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.

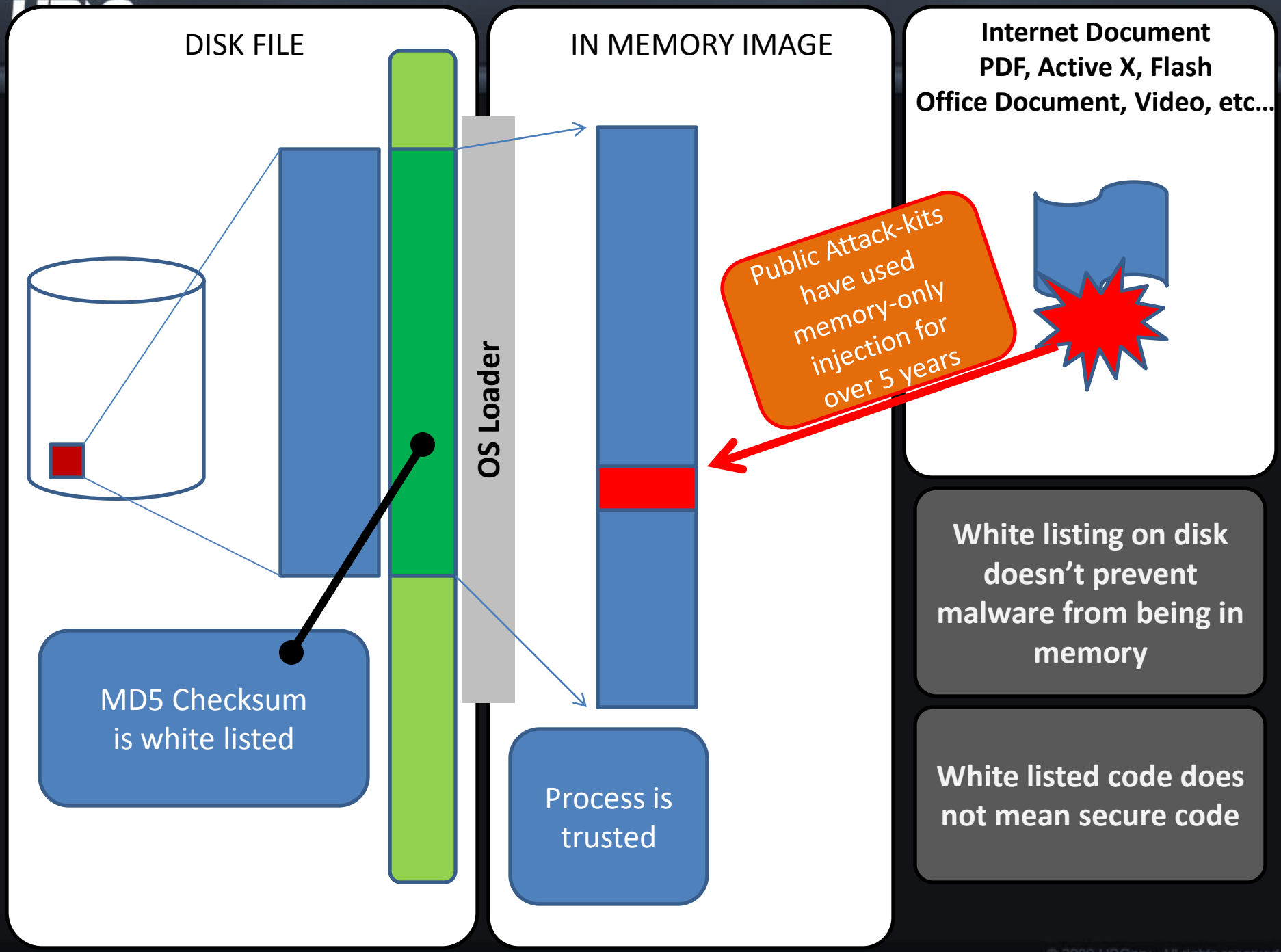
© 2009 HBGary. All rights reserved.

HBGary
DETECT. DIAGNOSE. RESPOND.

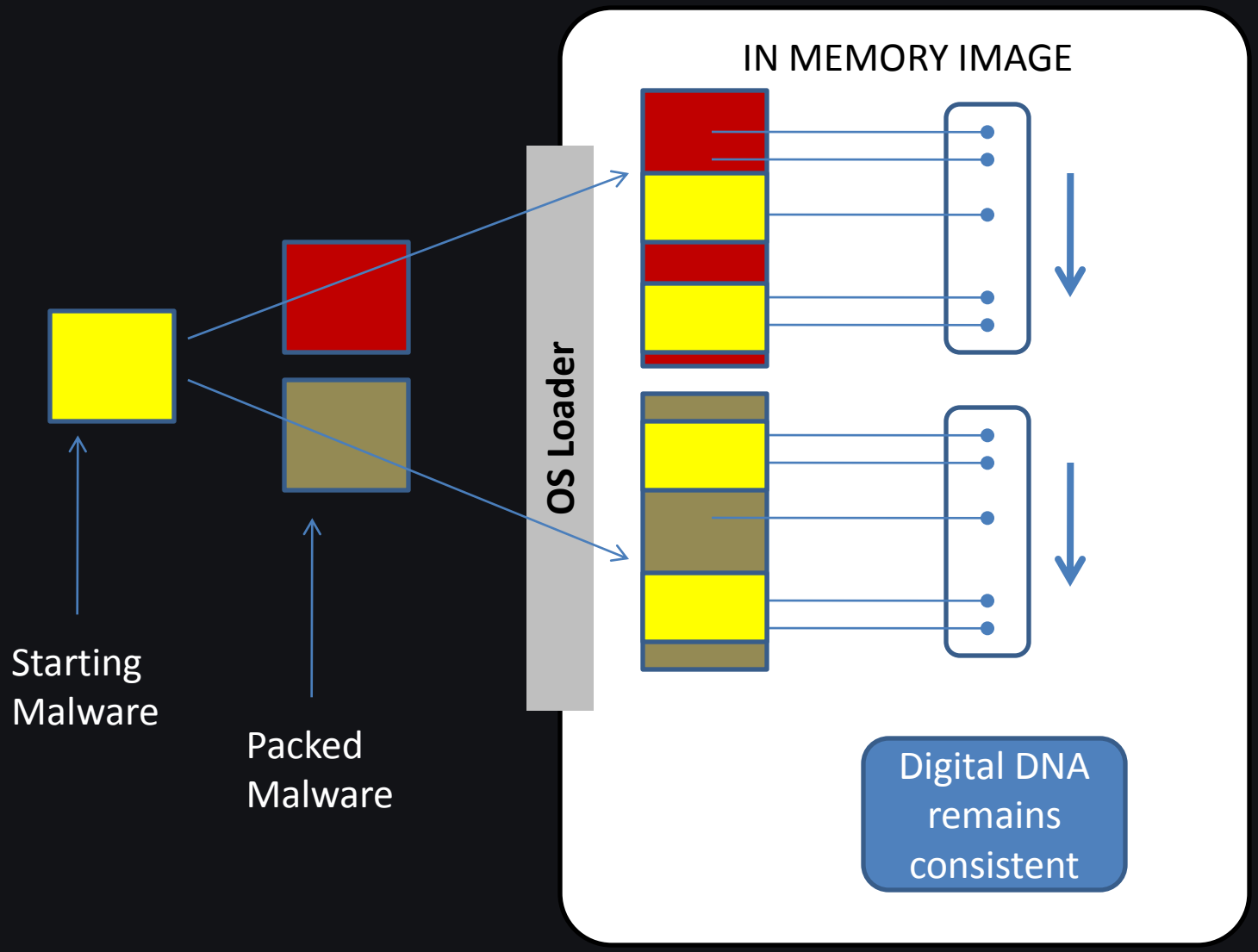
Digital DNA™ (in Memory)
vs.
Disk Based Hashing, Signatures, and other schematic approaches



© 2009 HBGary. All rights reserved.



© 2009 HBGary. All rights reserved.



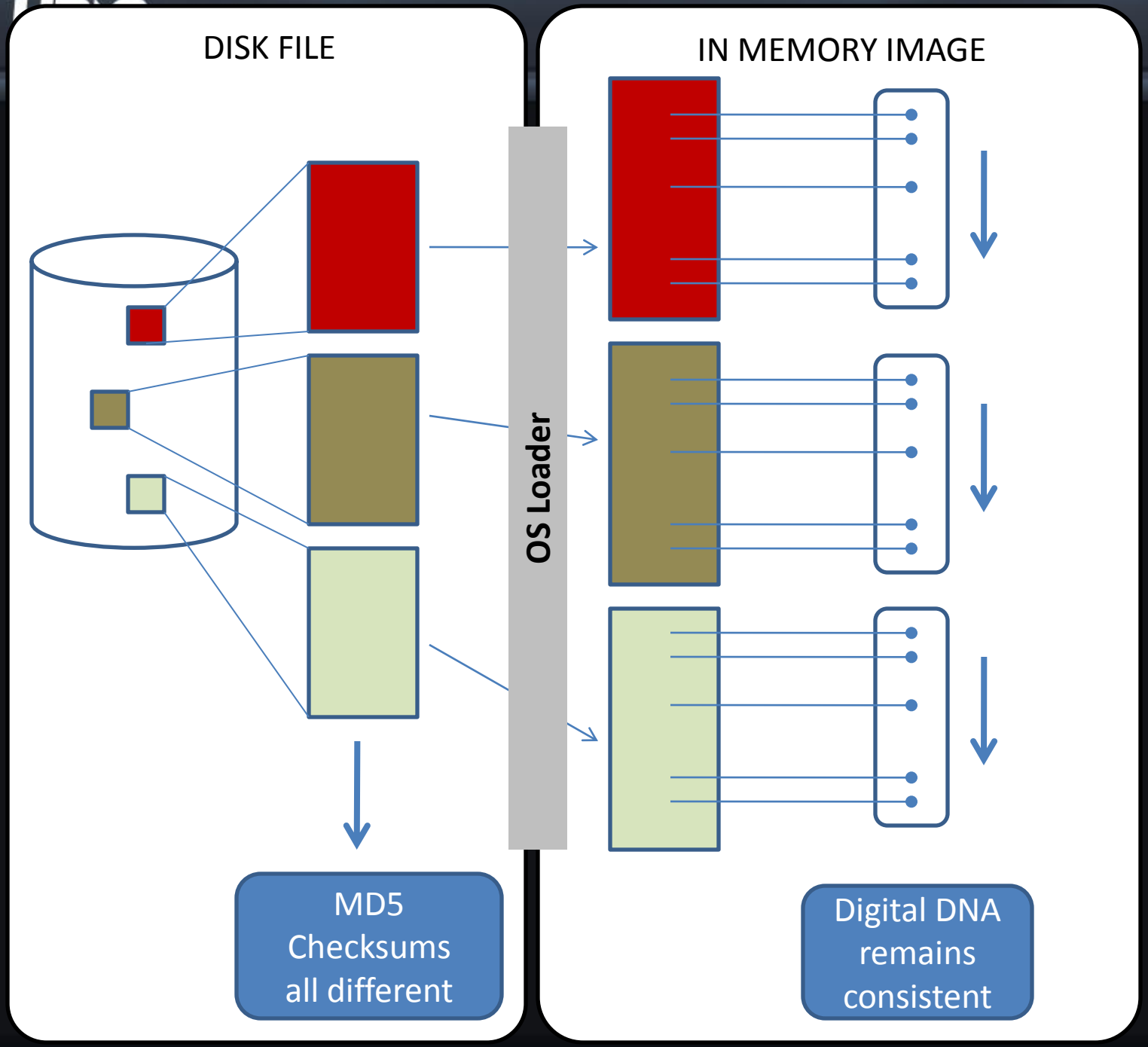
Packer #1

Packer #2

Decrypted Original

Digital DNA defeats packers

© 2009 HBGary. All rights reserved.

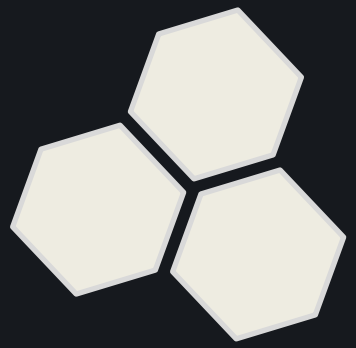


Same malware compiled in three different ways

© 2009 HBGary. All rights reserved.

Compromised computers…

Now what?



© 2009 HBGary. All rights reserved.

HBGary

DETECT. DIAGNOSE. RESPOND.

Active Defense™

Alert!

ActiveDefense
Management Console

Wednesday, April 7, 2010

ork > Systems > Detail

Detail > TESTNODE-3

Modules

ing page 1 of 44 (877 items) Page 1

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	

© 2009 HBGary. All rights reserved.

Hmm..

https://hbserver - Module Detail - Microsoft Internet Explorer

HBGary DETECT. DIAGNOSE. RESPOND.

ActiveDefense Management Console

Module Detail

Type	Module
Module	memorymod-pe-0x00090000-0x0018f000
Process	wmiprvse.exe
Digital DNA Score	75.0
Digital DNA Sequence	00 94 15 00 6E F6 80 80 00 80 80 01 80 80 02 80 80 08

Code	Trait Description
80 01	This package appears to have packer characteristics: Suspicious Entry Section w/ Data Sections
80 02	This package appears to have packer characteristics: Suspicious Non-Standard Section Names
80 08	This appears to be a hidden module, possibly injected.
80 00	This
94 15	The
6E F6	The

le, possibly injected.

ker characteristics: Sus

Done

Trusted sites

ActiveDefense Management Console

Wednesday, April 7, 2010

ork > Systems > De

Detail > TESTNODE-3

Modules

ing page 1 of 44 (877 items)

Page 1

Process Name	Score	Livebin
wmiprvse.exe	75.0	
System	37.8	
svchost.exe	30.0	
ddna.exe	22.4	
Unknown	19.0	
System	19.0	
explorer.exe	14.0	
svchost.exe	13.0	
ddna.exe	9.9	
taskmgr.exe	8.0	

© 2009 HBGary. All rights reserved.

Active Defense Queries

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

© 2009 HBGary. All rights reserved.

HBGary
DETECT. DIAGNOSE. RESPOND.

Active Defense Queries

Reports > Query Builder

Query Name: A Enter a query description here... System B Public C

Where

D LastResult.Module.Score = in genome Any Genome E

or Name contains

Add Another Field F

And Where

Name is exactly

Add Another Field

Add Another Criteria Block G

H

Cancel Save Query

© 2009 HBGary. All rights reserved.

HBGary
DETECT. DIAGNOSE. RESPOND.

Active Defense Queries

QUERY: “detect use of password hash dumping”

Physmem.BinaryData **CONTAINS PATTERN** “[redacted]

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**

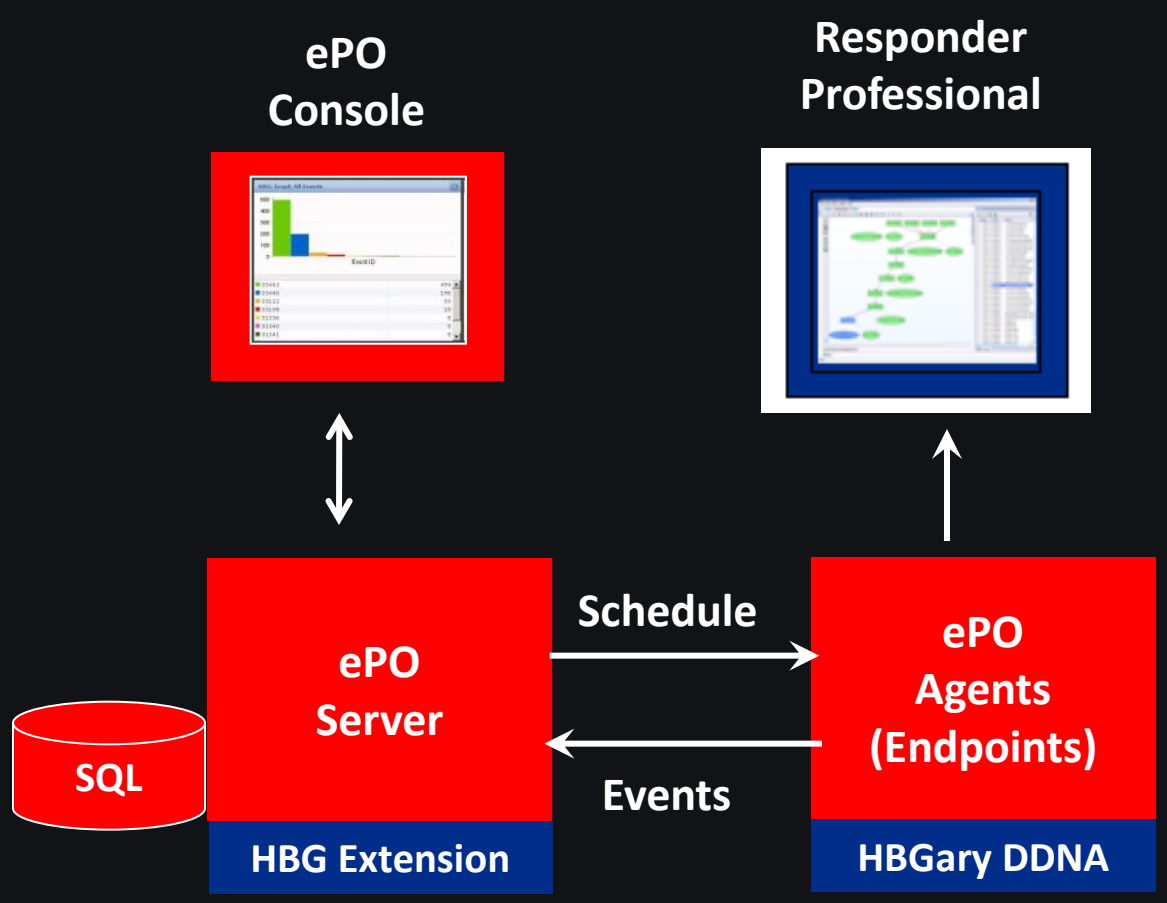
© 2009 HBGary. All rights reserved.

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

© 2009 HBGary. All rights reserved.

Integration with McAfee ePO



© 2009 HBGary. All rights reserved.

HBGary
DETECT. DIAGNOSE. RESPOND.

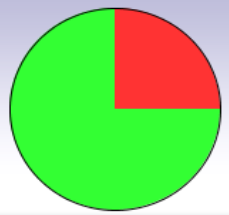
Server: mcserver | Time: 11/26/08 12:51 PM PST | User: admin Log Off

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 (	iimo.sys	System		92.7
01 40 DA 04 2B 69 05 60 0B 05 7E F2 (	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 (	vmnat.exe	vmnat.exe		25.7
07 CD E3 05 4F 90 05 A8 F1 05 89 E4 (	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 (	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 com
89 B9	This driver uses trap frames, this is related to interrupt hooking. Interrupt hooks are a com
5F FD	This driver uses trap frames, this is related to interrupt hooking. Interrupt hooks are a com
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.

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

Trait Search

Trait Sequence: 0B 8A C2 05 0F 51 03 0F 64 05 01 3A

Threshold: 80 %

Search | Cancel

Severity	Name	Score
	HBGARY-PMLAPPY	92.7
	MCSERVER	-16.0
	HBGARY-FC5D70D2	-16.0
	_	-16.0

Fuzzy Search

Module Explorer

Machine: HBGARY-PMLAPPY

Modules

Sequence	Module	Process	Severity	Score
0B 8A C2 05 0F 51 03 0F 64 05 01 3A (	iimo.sys	System		92.7
01 40 DA 04 2B 69 05 60 0B 05 7E F2 (	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 (	vmnat.exe	vmnat.exe		25.7
07 CD E3 05 4F 90 05 A8 F1 05 89 E4 (	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 (	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

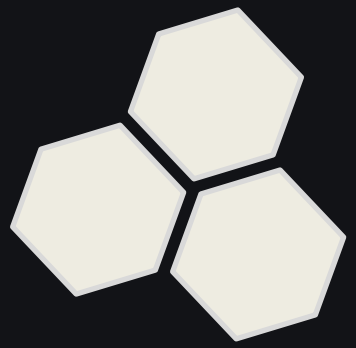
© 2009 HBGary. All rights reserved.

HBGary
DETECT. DIAGNOSE. RESPOND.

Responder

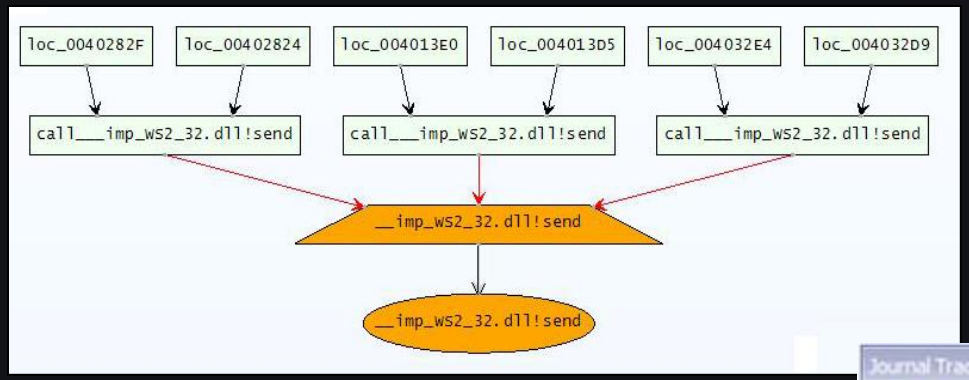
HBGary Responder Professional

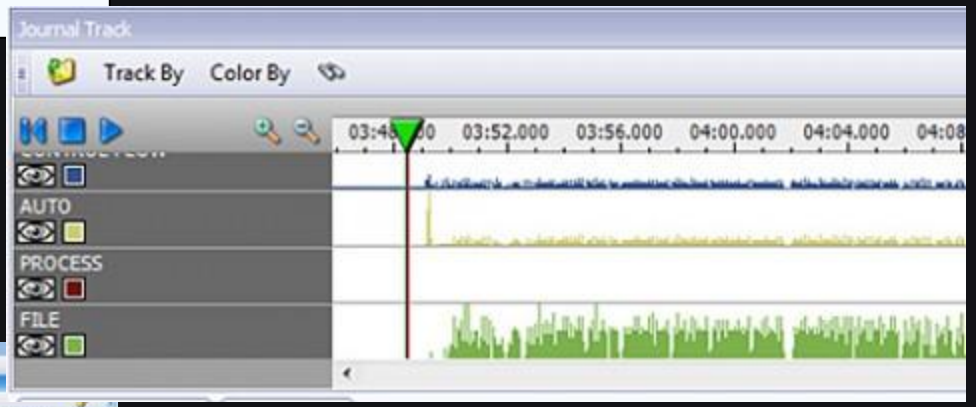
- Standalone system for incident response
- Memory forensics
- Malware reverse engineering
  - Static and dynamic analysis
- Digital DNA module
- REcon module

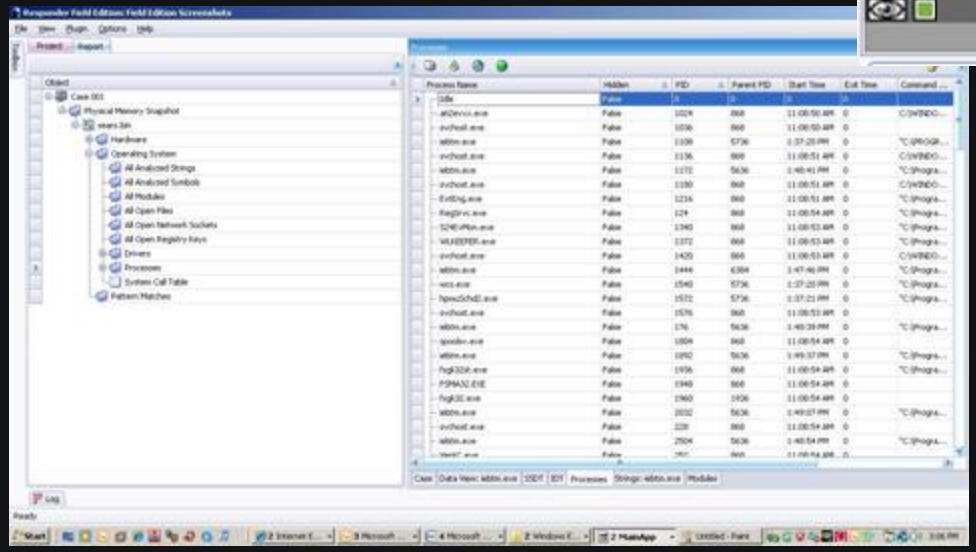


© 2009 HBGary. All rights reserved.

Responder Professional







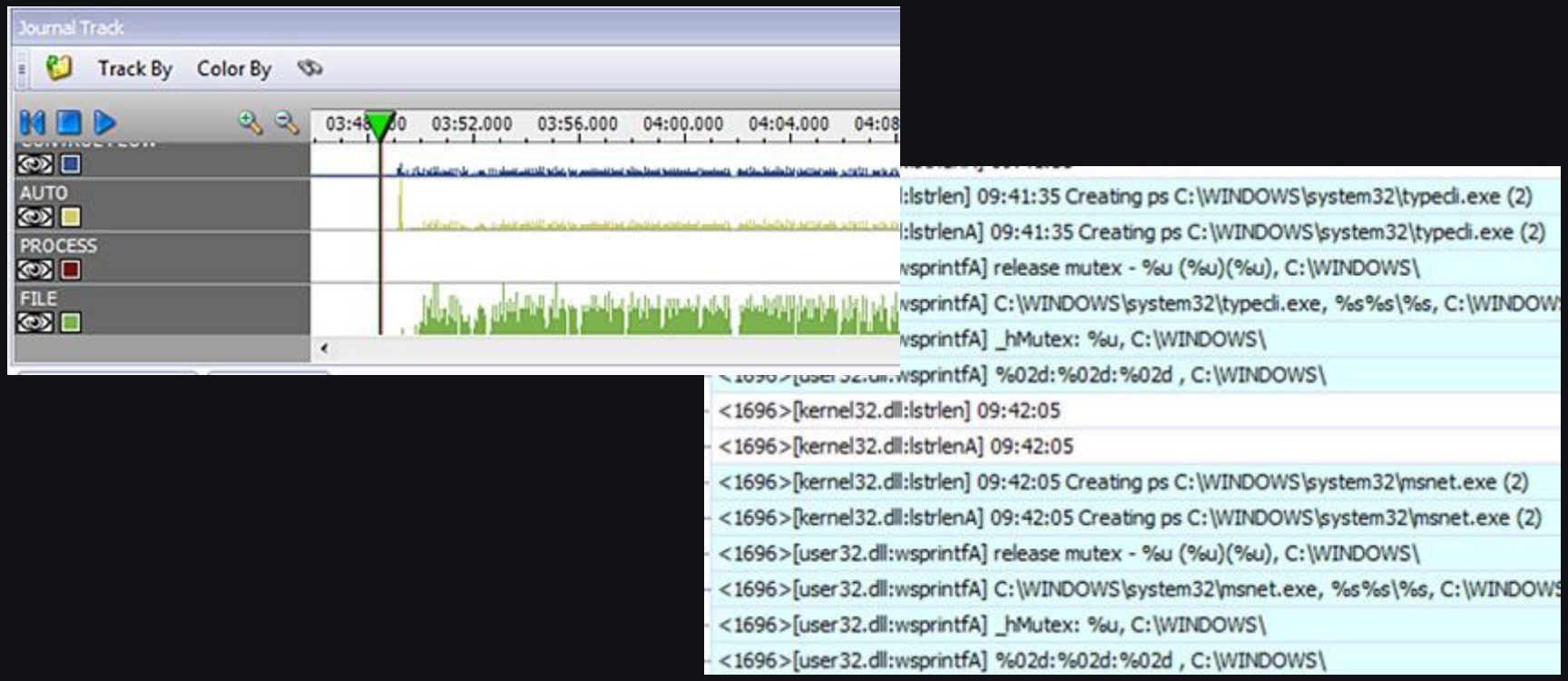
© 2009 HBGary. All rights reserved.

HBGary
DETECT. DIAGNOSE. RESPOND.

REcon

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.



© 2009 HBGary. All rights reserved.

HBGary

DETECT. DIAGNOSE. RESPOND.

Advanced Discussion: How HBGary maintains DDNA with Threat Intelligence

HBGary
DETECT. DIAGNOSE. RESPOND.

Intelligence Feed

Partnership Feed Agreements

Feed Processor

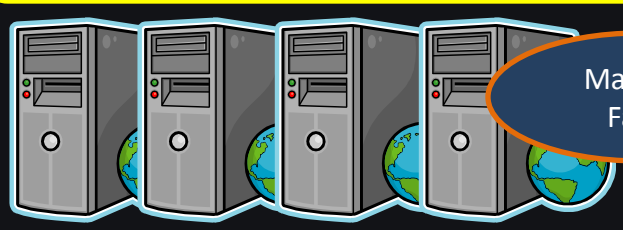
Cyveillance®

shadowserver

AV. TEST

McAfee®

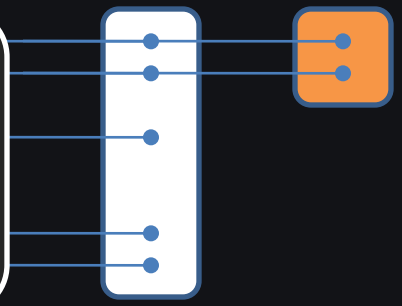
Sources



Machine Farm

Meta Data

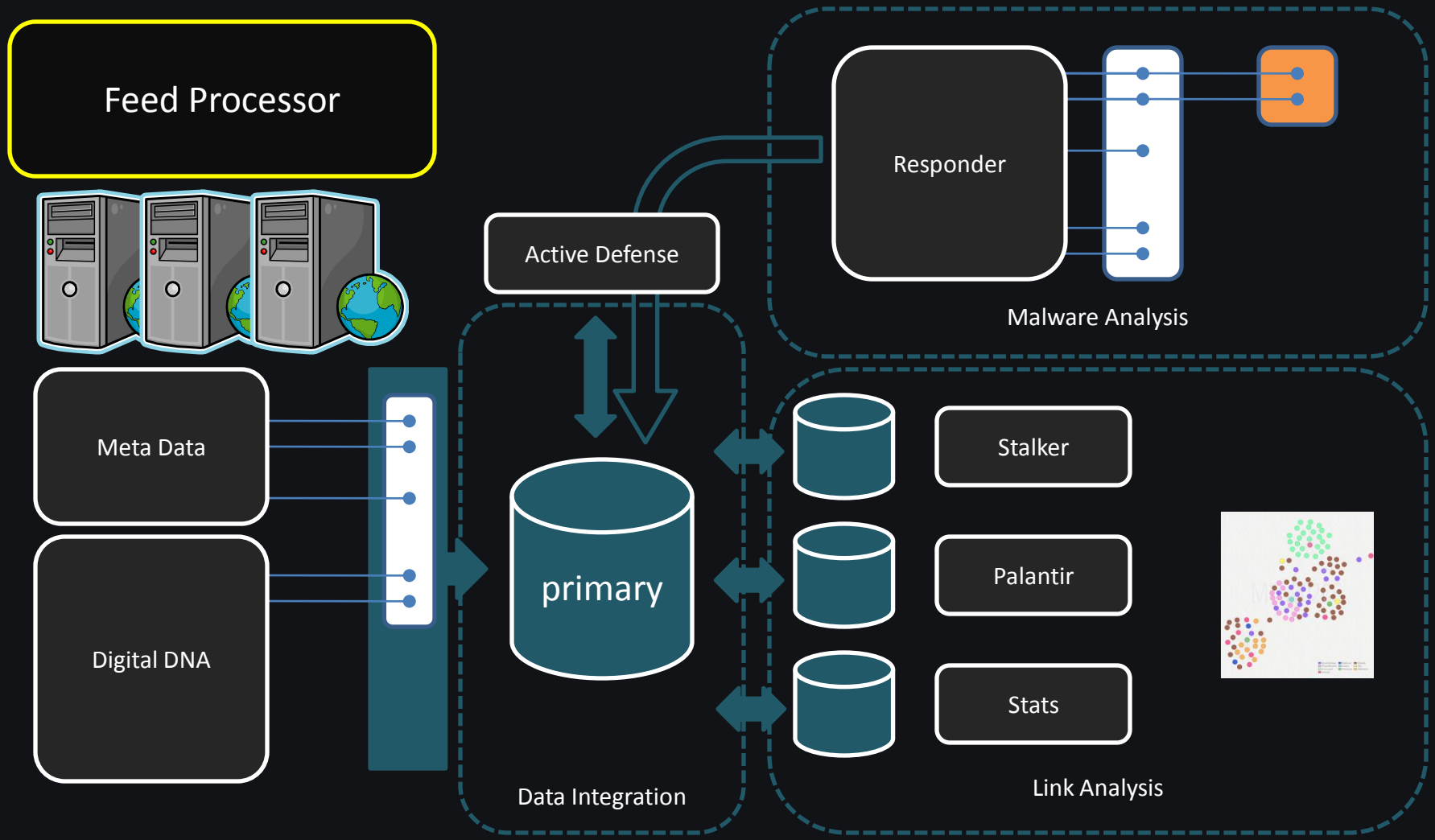
Digital DNA



© 2009 HBGary. All rights reserved.

HBGary
DETECT. DIAGNOSE. RESPOND.

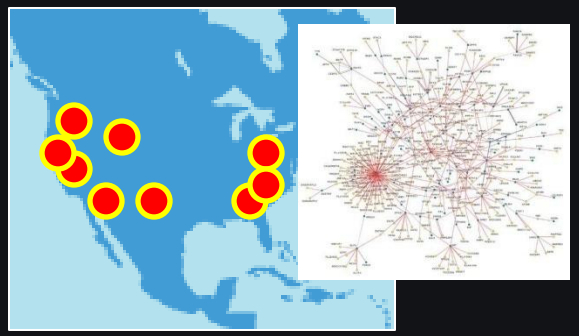
From raw data to intelligence

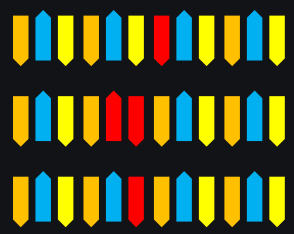


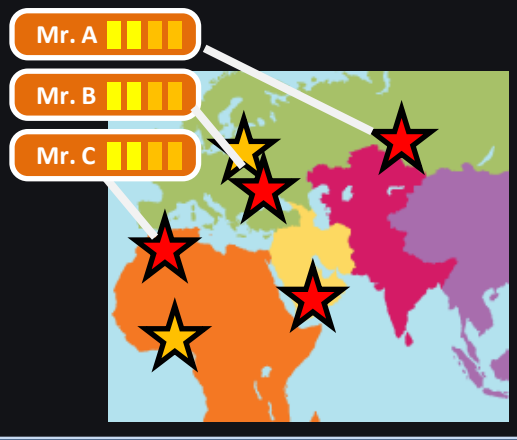
© 2009 HBGary. All rights reserved.

HBGary
DETECT. DIAGNOSE. RESPOND.

Ops path







Malware Attack 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

Digital DNA™

Development idioms are fingerprinted. Malware is classified into attribution domains. Special attention is placed on:
- Specialized attacks
- Targeted attacks
- Newly emergent methods

Active Threat Tracking

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

© 2009 HBGary. All rights reserved.

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 B 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 Glob

DETECT. DIAGNOSE. RESPOND.

HOME ADMINISTRATION

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 tec

Hit Report

Malware

Trusted

Unknown

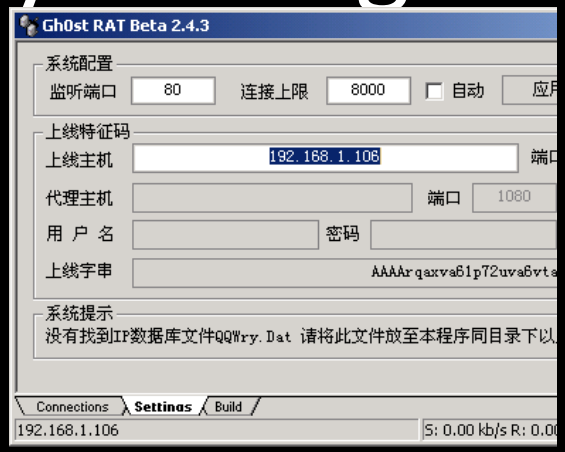
Factor / Group / Subgroup		
Installation and Deployment	14	87.5%
Code Injection	11	68.8%
Process Memory		50.0%
Thread Injection		12.5%
Process Enumeration		43.8%
Temp Files Dropped in RAM or File System		18.8%
Reboot Survival		56.3%
Registered Service		25.0%
Explorer AddOn		18.8%
INI Files		12.5%
Development		62.5%
Compression		50.0%
Self Defense		68.8%
File Time Modifications	3	18.8%
Evidence Removal	2	12.5%
Sabotage	5	31.3%
Antivirus	0	-- %
Desktop Firewall	0	-- %
Anti-virus	5	31.3%
Communications	13	81.3%
Email Protocol	2	12.5%
SMTP	2	12.5%
IRC Protocol	1	6.3%

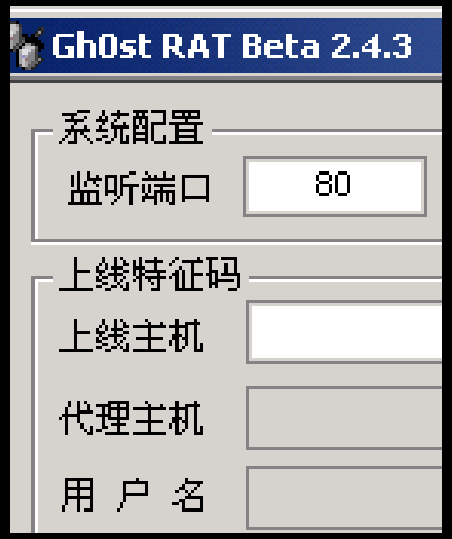
Over 5,000 Traits are categorized into Factor, Group, and Subgroup.

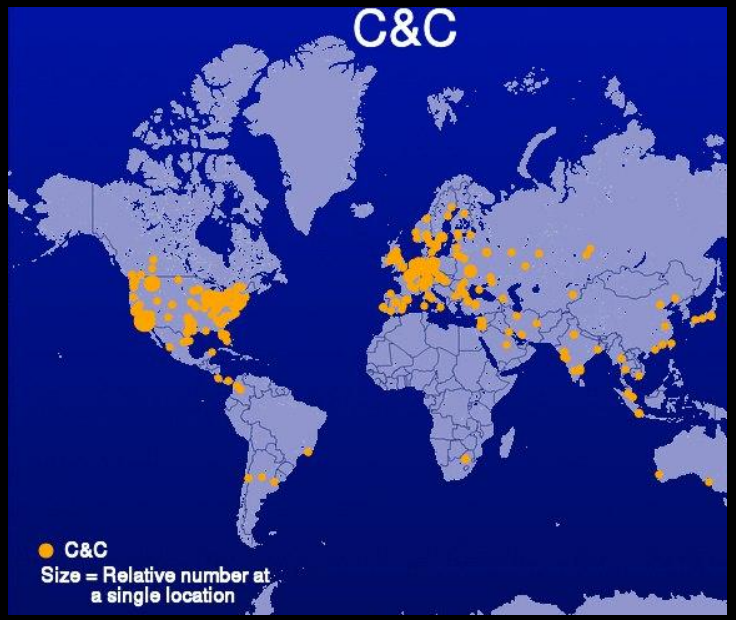
This is our "Genome"

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',                                                  //Те
define('ONLINE_TIME_MIN',                                          );   //Ми
define('DEFAULT_LANGUAGE'                                               //Яз
define('THEME_PATH',        'theme');                                   //Па

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

//Сессия, куки.
define('COOKIE_USER',       'p');                       //Имя пользоват
define('COOKIE_PASS',       'u');                       //Пароль пользо
define('COOKIE_LIVETIME',   CURRENT_TIME + 2592000);    //Время жизни
define('COOKIE_SESSION',    'ref');                     //Переменная д
define('SESSION_LIVETIME',  CURRENT_TIME + 1300);       //Время жизни

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

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

Константы.

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…

```
00000140  3D B4 3B 3B B3 46 46 B7  D0 D0 EC CB CB EA 7C 7C  =´;;³FF·ÐÐìËËê||
00000150  CC BF BF E6 7A 7A CB 48  48 B8 B5 B5 E2 36 36 B1  Ì¿¿æzzËHH¸µµâ66±
00000160  75 75 C9 [illegible] E4 42  uuÉ::³▌▌Ð▌▌Ñ¼¼äB
00000170  42 B6 94 [illegible] 00 00  B¶▌▌ÕWW¾▌▌Ø,,-..
00000180  00 00 00 [illegible] FF 0B  ..........!ÿ.
00000190  4E 45 54 [illegible] 00 00  NETSCAPE2.0.....
000001A0  21 FE 1D [illegible] 47 49  !þ.Built with GI
000001B0  46 20 4D [illegible] 2E 30  F Movie Gear 4.0
000001C0  00 21 FE [illegible] 51 78  .!þ.Made by Ajax
000001D0  4C 6F 61 [illegible] 0A 00  Load.info.!ù....
000001E0  00 00 2C [illegible] 80 00  ..,.... . ...ÿ▌.
000001F0  82 83 84 [illegible] 90 91  ▌▌▌▌▌▌▌▌▌▌▌.▌..´
00000200  92 84 0B [illegible] 3A 3B  ´▌.964▌▌..!▌.5:;
00000210  12 99 0A [illegible] 90 0B  .▌..."▌.";=5▌..
00000220  11 19 18 19 0E 00 14 1A  AD 3F 82 0B 37 40 02 8E  .........-?▌.7@.▌
00000230  02 12 1A 19 29 18 32 00  36 3C 3E 28 00 42 28 D1  ....).2.6<>(.B(Ñ
```

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

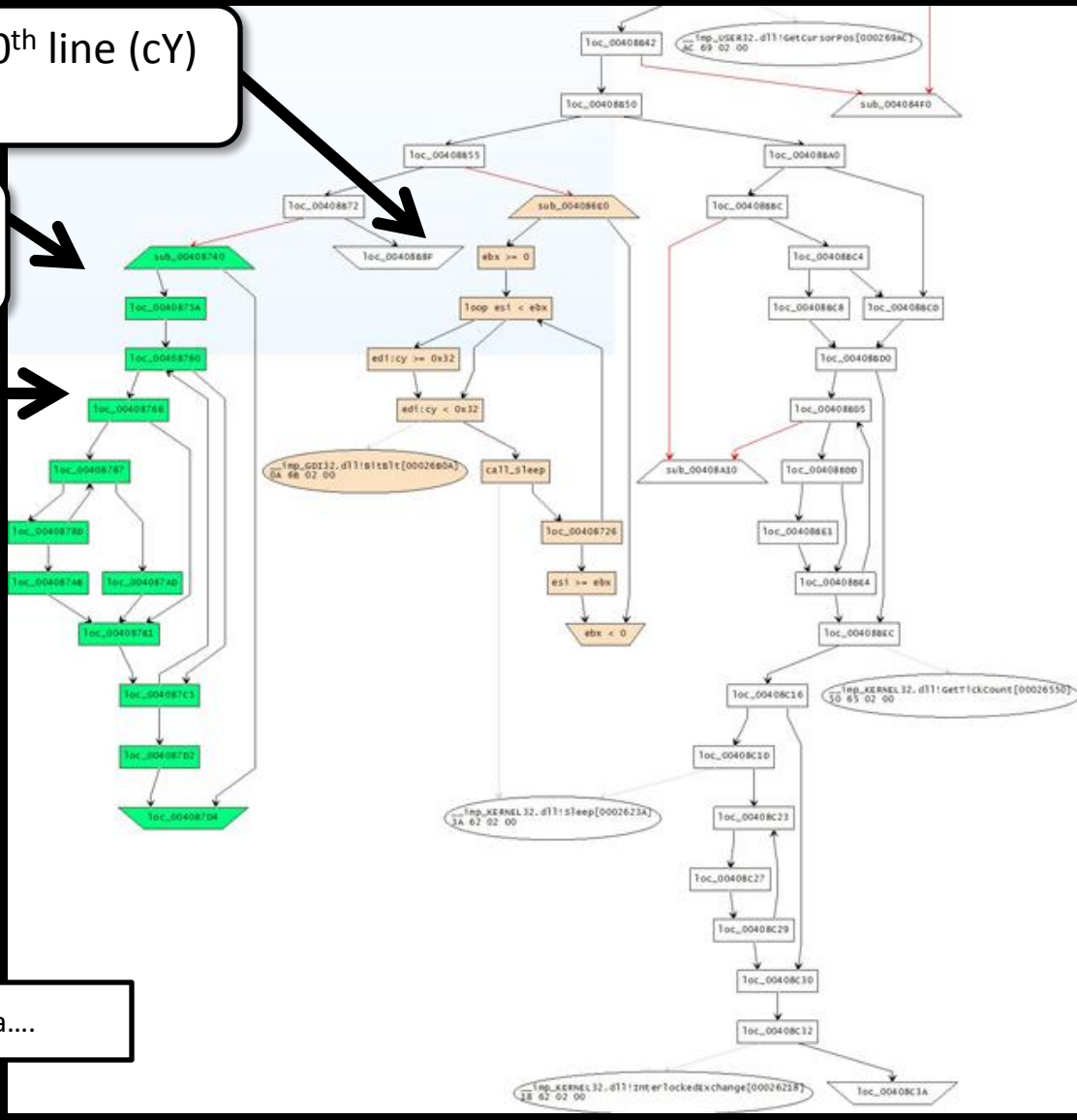
GhostNet: Screen Capture Algorithm

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

Reads screenshot data, creates a special DIFF buffer

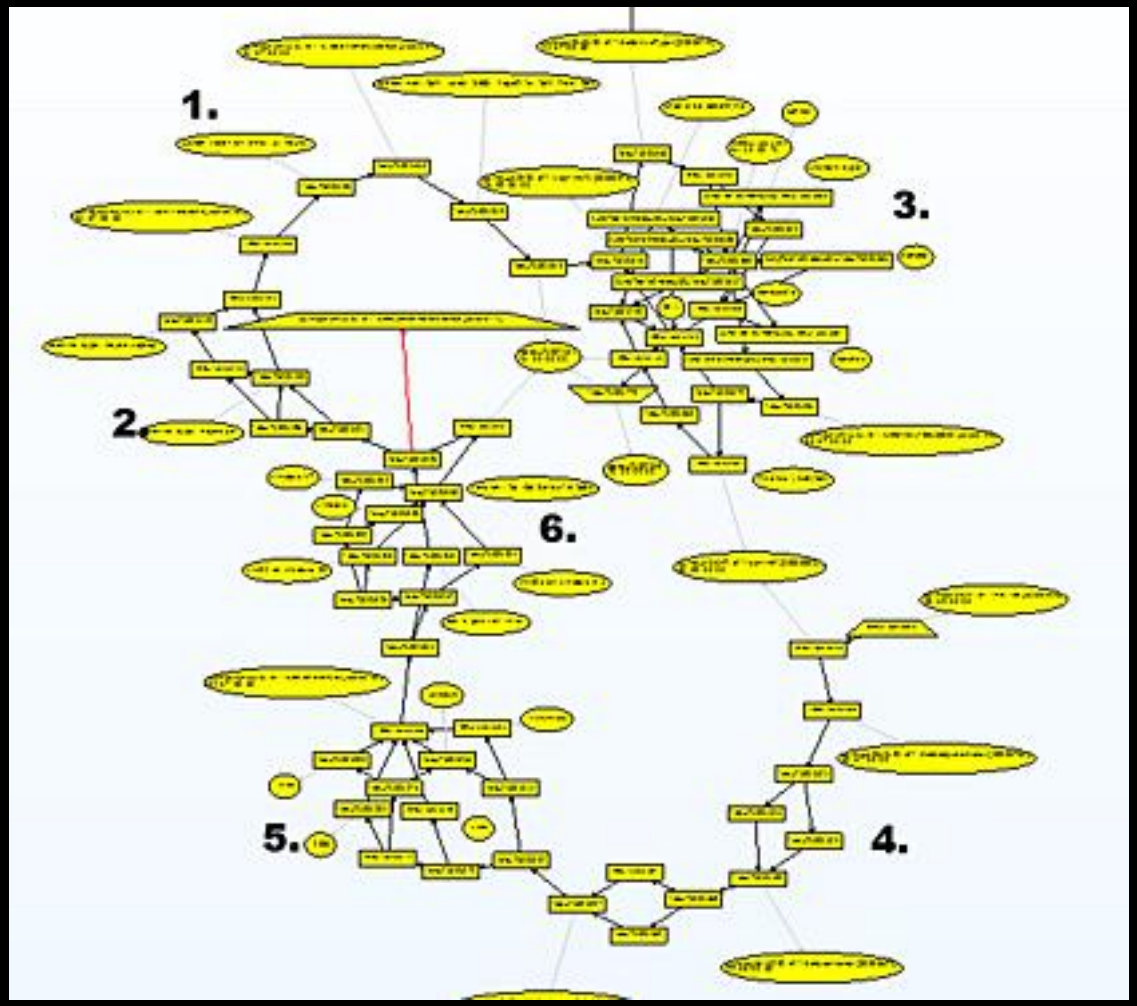
LOOP: Compare new screenshot to previous, 4 bytes at a time

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



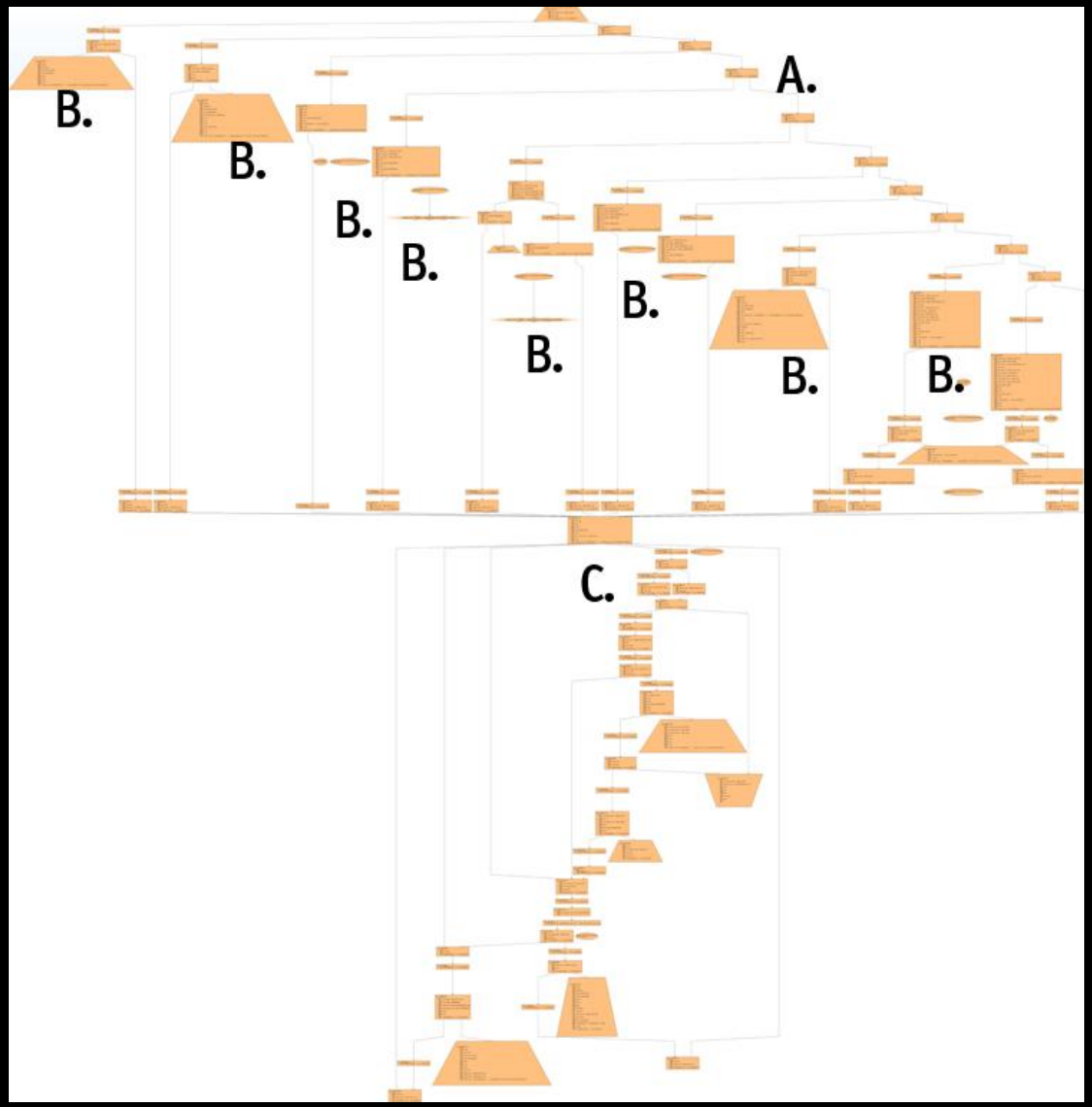
Offset in screenshot	Len in bytes	Data….

‘Soysauce’ C&C Hello Message



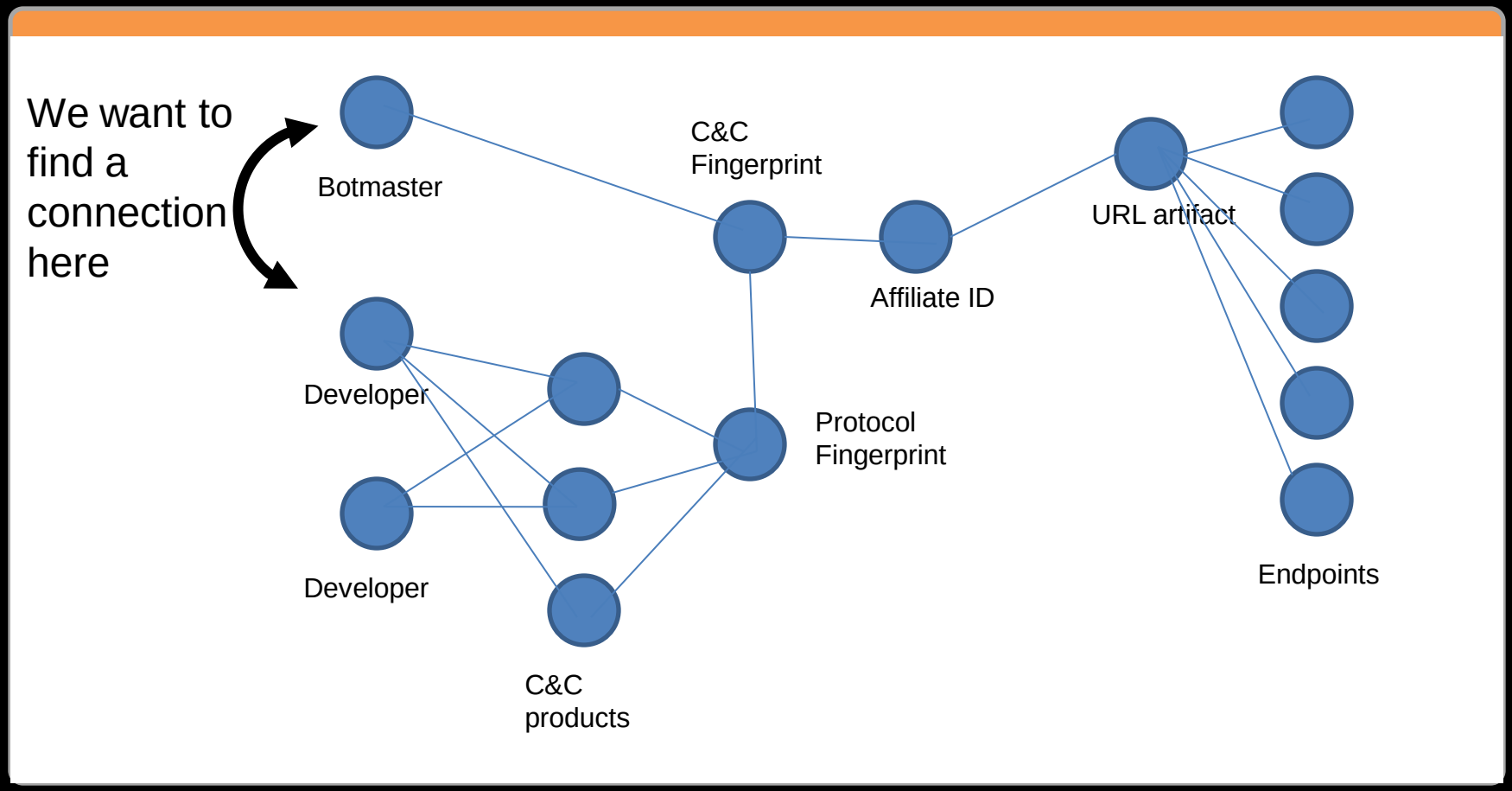
1) this queries the uptime of the machine..
2) checks whether it's a laptop or desktop machine...
3) enumerates all the drives attached to the system, including USB and network...
4) gets the windows username and computername...
5) gets the CPU info... and finally,
6) the version and build number of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

Aurora C&C parser



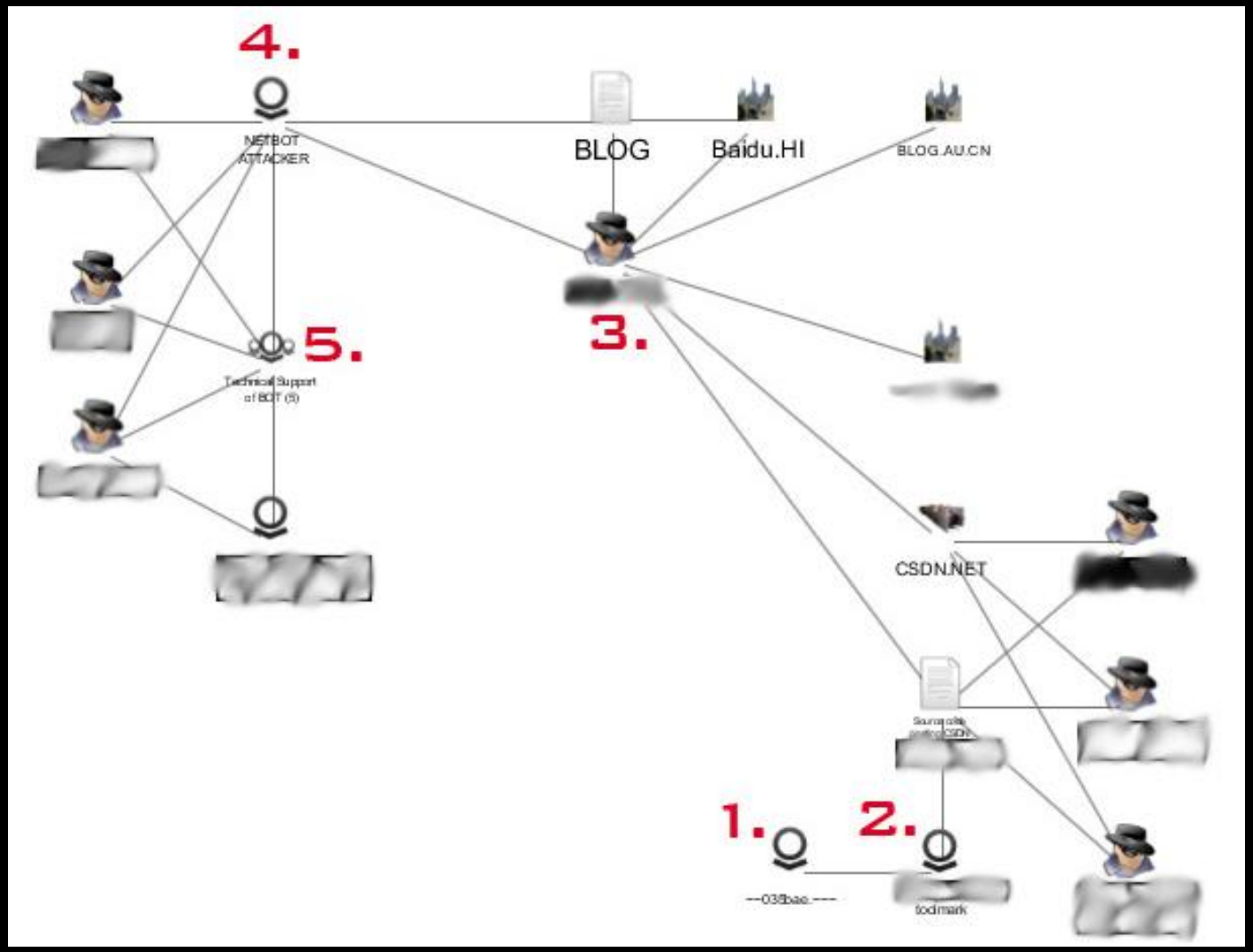
A) Command is stored as a number, not text. It is checked here.
B) Each individual command handler is clearly visible below the numerical check
C) After the command handler processes the command, the result is sent back to the C&C server

Link Analysis



Link Analysis

Example: Link Analysis with Palantir™



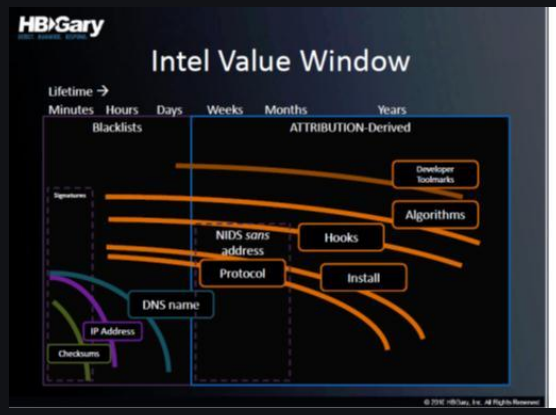
1. Implant
2. Forensic Toolmark specific to Implant
3. Searching the ‘Net reveals source code that leads to Actor
4. Actor is supplying a backdoor
5. Group of people asking for technical support on their copies of the backdoor

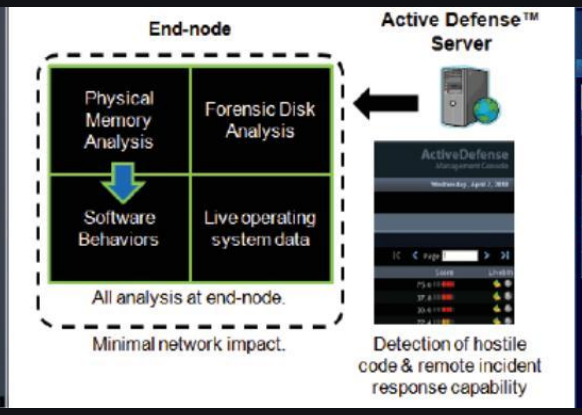
HBGary
DETECT. DIAGNOSE. RESPOND.

Questions?

Product Overview

Product Demo





© 2009 HBGary. All rights reserved.

Conclusion

- We look forward to working with you throughout this process.

Thank You!

© 2009 HBGary. All rights reserved.