From: "Aaron Barr" <aaron@hbgary.com>
To: "Bob Slapnik" <bob@hbgary.com>
Sent: Thursday, April 29, 2010 7:57 AM
Attach: Threat Monitoring Center-3.ppt
Subject: Re: Slides so far

On Apr 29, 2010, at 8:46 AM, Bob Slapnik wrote:

> Aaron,
>
> You sent me some kind of weir file type. I can read ppt or pdf files, not a
> .key file type.
>
> Bob
>
>
> -----Original Message-----
> From: Aaron Barr [mailto:aaron@hbgary.com]
> Sent: Wednesday, April 28, 2010 10:46 PM
> To: Bob Slapnik
> Subject: Re: Slides so far
>
>
>
> I still have some work on these but wanted your input.
>
> I think based on your information more needs to be added as well.
>
> Aaron
>
> On Apr 28, 2010, at 4:25 PM, Bob Slapnik wrote:
>
>> Aaron,
>>
>> I could not see any slides. Please send as powerpoint file or as pdf.
>>
>> Bob
>>
>> -----Original Message-----
>> From: Aaron Barr [mailto:aaron@hbgary.com]
>> Sent: Wednesday, April 28, 2010 3:09 PM
>> To: Bob Slapnik
>> Subject: Slides so far
>>
>> Hey Bob,
>>
>> Tell me what you think so far. Still working on them.
>>
>> Aaron Barr
>> CEO
>> HBGary Federal Inc.

>>
>>
>> No virus found in this incoming message.
>> Checked by AVG - www.avg.com
>> Version: 9.0.814 / Virus Database: 271.1.1/2840 - Release Date:
>> 04/28/10 02:27:00
>>
>
> Aaron Barr
> CEO
> HBGary Federal Inc.
>
>
> No virus found in this incoming message.
> Checked by AVG - www.avg.com
> Version: 9.0.814 / Virus Database: 271.1.1/2840 - Release Date: 04/29/10
> 02:27:00
> <Threat Monitoring Center-3.key>

Aaron Barr
CEO
HBGary Federal Inc.

HBGary
Risk Intelligence

HBGary Goals

- Deliver a set of products and service that improve the speed and accuracy of incident response and malware analysis. Building proactive threat detection capabilities.
- Tools that accomplish the vision:
  - DDNA - detection and scoring of specimens based on behavior using a genome of codified malware traits.
  - Responder - Streamlined malware analysis. Lowers the price point for malware analysis staff.
  - REcon - Runtime tracing and collection of low level data.
  - Active Defense - Enterprise management of DDNA.
  - TMC - Automated volume processing of malware.
- Services expertly qualified on HBGary and Partner tools.

HBGary
Risk Intelligence

Product Placement

- TMC built for the larger Threat Centers, SOCs, CERTs, to process malware samples and develop threat intelligence. Integration with products such as Palantir, EGS, Open Source, SIGINT.
- Active Defense - Built for Enterprise malware detection and protection. Integration point with other detection and protection capabilities such as Fidelis, SourceFire, Snort. Manages the deployment of DDNA to the end points and provide enterprise search capabilities of threat artifacts.
- DDNA - NexGen Malware detection using behavior analysis. 1000s of Keyloggers - ~10 ways to log key strokes.
- Responder - Highly efficient memory analysis tool.
- REcon - Very granular runtime tracing and collection tool.

HBGary
Risk Intelligence

Threat Monitoring Center

- Initial deployment to deliver advanced capability for incident mitigation and triage of incoming specimens
  - Automated prioritization of incoming samples for more advanced analysis using threat scores for probability of malware (DDNA)
- Integrate data with more advanced malware and threat analysis framework and other data sources to build more automated Cyber Threat Profiles and Scenarios.
  - Tight integration with Responder and REcon

HBGary
Risk Intelligence

Threat Monitoring Center

- Focus on quick deployment of analysis capability for one full time person
  - First deployment after two development iterations (4 weeks)
- Phase I analysis capabilities will be largely emergent, back-driving requirements
  - Technology requirements will change rapidly over first 6 months as new use cases are learned
  - TMC will be hand built and replicated, one for HBGary and one for HBGary Federal

HBGary

Intelligence Feed

Partnership Feed Agreements

Feed Processor

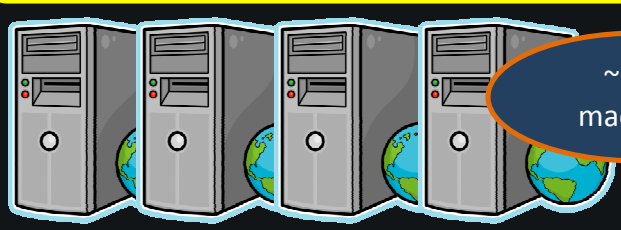
Cyveillance

shadowserver

AV-TEST

McAfee

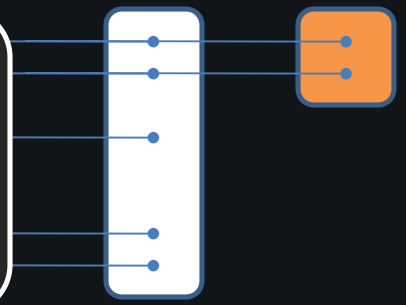
$10K / yr



~ $8K machines

Meta Data

Digital DNA



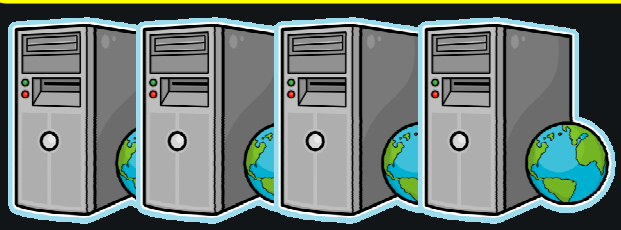
HBGary

Intelligence Feed

Additional Feed Sources

http://www.safer-networking.org/en/threats/
http://www.emergingthreats.net/rules/
http://www.symantec.com/business/security_response/threatexplorer/
http://code.mwcollect.org/
http://nepenthes.carnivore.it/
http://www.offensivecomputing.net/
http://www.threatexpert.com/
http://www.support-intelligence.com
http://www.threatstop.com
Many more….

Feed Processor



Meta Data

Digital DNA

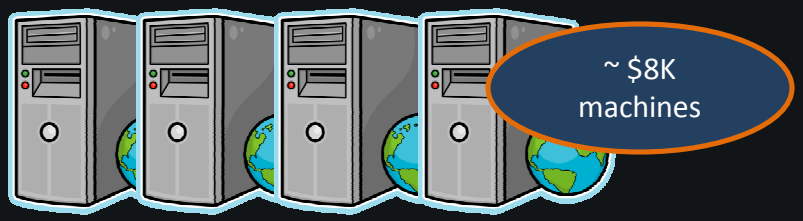
HBGary
Risk Intelligence

Intelligence Feed

AV Updates as Feed Source

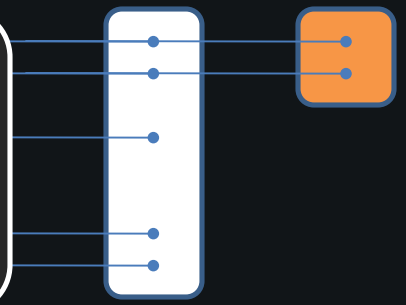
avast! Free 5.0
AVG Anti-Virus 9.0
AVIRA AntiVir Premium 9
BitDefender Antivirus 2010
eScan Anti-Virus 10
ESET NOD32 Anti-Virus 4.0
F-Secure Anti-Virus 2010
G DATA AntiVirus 2010
Kaspersky Anti-Virus 2010
Kingsoft Antivirus 2009+
McAfee VirusScan Plus 2010
Microsoft Security Essentials 1.0
Norman Antivirus & Anti-Spyware 7.30
Sophos Anti-Virus 9.0
Symantec Norton Anti-Virus 2010
TrustPort Antivirus 2010

Feed Processor



Meta Data

Digital DNA

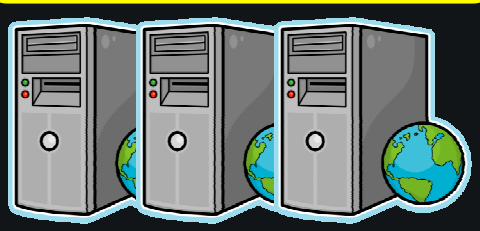


HBGary

Risk Intelligence

From raw data to intelligence

Feed Processor



Active Defense

Responder

Malware Analysis

Meta Data

Digital DNA

primary

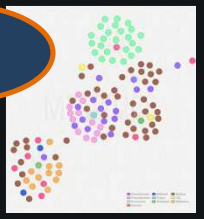
4g

Maltego

$12K

Palantir

Dev free



i2 Analyst Workstation

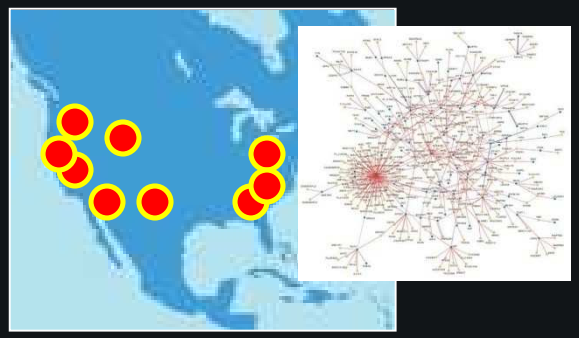
$4K

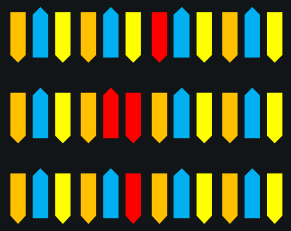
Data Integration

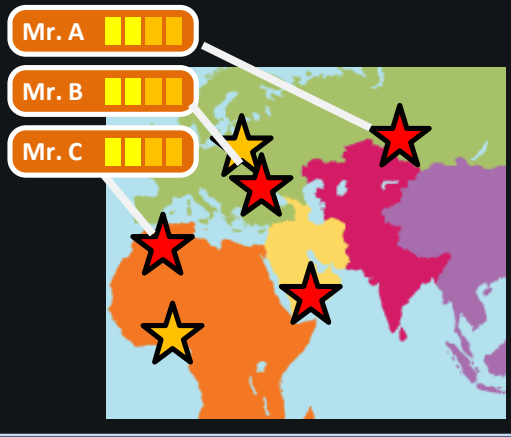
Link Analysis

HBGary
Risk Intelligence

Ops path



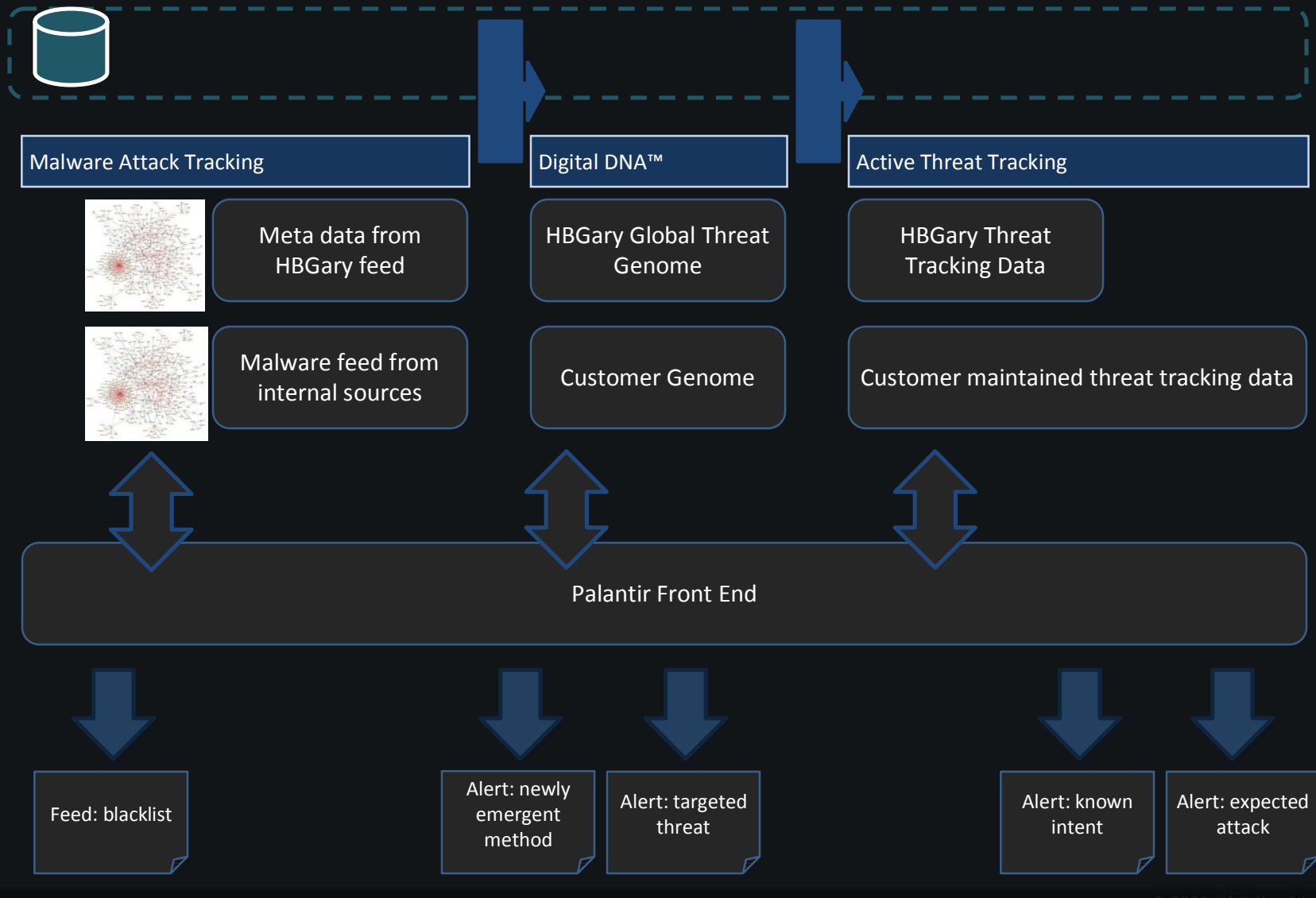




Malware Attack Tracking	Digital DNA™	Active Threat Tracking
Detect relevant attacks in progress. Determine the scope of the attack. Focus is placed on • Botnet / Web / Spam Distribution systems • Potentially targeted spear/whalefishing • Internal network infections at customer sites	Development idioms 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
Risk Intelligence

Cyber Command Integration



HBGary
Risk Intelligence

Integration

- User Defined Traits
- Developed SNORT Signatures