HBGary
Detecting Tomorrow's Threats Today

ManTech
International Corporation

FORTUNE 50 CASE STUDY

Industry:
Fortune 50 Company

Headquarters:
Eastern USA

Employees:
Over 100,000

Objective: Respond and protect against targeted attacks

Solution: HBGary Managed Services using Active Defense™ with Digital DNA

Key Benefit: "HBGary Active Defense™ is on the frontline of our digital investigations. It is a fast way to spot malware and detect compromised machines throughout the network."

> *"We identified 40 new pieces of malware within first month of Active Defense™ deployment."*

> *"The fact that the HBGary Managed Services team can remotely protect our network is a huge benefit."*

Security Challenge:
IT security staff is understaffed and needs help to combat targeted attacks.

Rollout:
The company rolled out Active Defense™ with Digital DNA to 20,000 end-nodes in April 2011. By July 2011, the company had rolled out the product to 50,000 end-nodes and currently the product is deployed over 70,000 end-nodes. The company hopes to roll it out throughout the rest of the company by end of this year. Currently, the company scans once a week.

APT Solution Selection Process:
In 2009, the company was first interested in HBGary's Responder™ Pro – "we liked its capability to do malware analysis in memory. We called it "AV for Memory." They also acquired yearly subscription to HBGary's Digital DNA technology. Based on its initial success with Responder™ Pro, the company decided to acquire Active Defense™ with Digital DNA after experiencing a significant security incident.

> *"We think HBGary's Digital DNA is a product of the future – the concept is very impressive."*

Why Active Defense™ with Digital DNA?

Detect Zero-day attacks

■ HBGary's Active Defense™ expertly detects zero-day attacks and the managed services team helps our team with whitelisting to further protect their network.

Determine scope of infection

■ The company has a large, diverse network across multiple business units; so it is critical, after an incident, to quickly determine whether the APT attacker has infected other parts of the enterprise. "Using Active Defense™, we can quickly scan for the attackers' tools and other artifacts determine scope of compromised machines throughout our network."

Expert malware analysis

■ Active Defense™ with Digital DNA allows us to quickly detect and "bucket" those threats that need immediate attention. "With a small IT security staff, it is critical that we prioritize our incident response." With Responder™ Pro, the company can do extensive malware analysis in physical memory to gain valuable threat intelligence to help mitigate risk to confidential information. HBGary Managed Services team does rapid response reverse engineering for difficult pieces of malware.