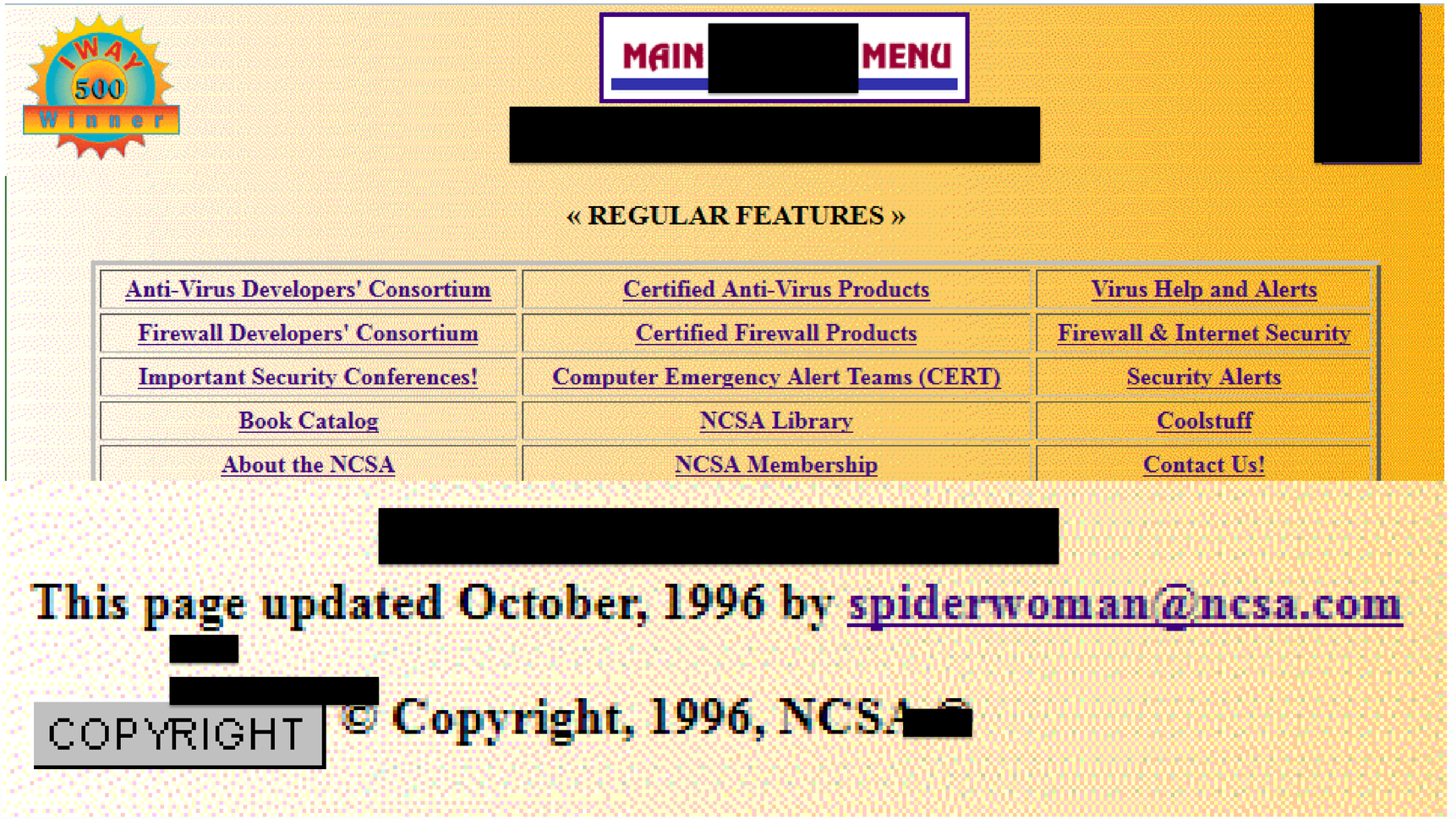
ENJOY SAFER TECHNOLOGY

# Big Data Security and Threat Sharing

Stephen Cobb


IWAY
500
Winner
MAIN [redacted] MENU
[redacted]
« REGULAR FEATURES »
Anti-Virus Developers' Consortium
Certified Anti-Virus Products
Virus Help and Alerts
Firewall Developers' Consortium
Certified Firewall Products
Firewall & Internet Security
Important Security Conferences!
Computer Emergency Alert Teams (CERT)
Security Alerts
Book Catalog
NCSA Library
Coolstuff
About the NCSA
NCSA Membership
Contact Us!
[redacted]
This page updated October, 1996 by spiderwoman@ncsa.com
[redacted]
COPYRIGHT
© Copyright, 1996, NCSA[redacted]

# Agenda

- Big Data Security
- BDS and threat discovery
- Challenges of threat data sharing
- AV industry experience
- Lessons learned
- Path forward

But first, let’s play:
Name That Threat!

# Name that Threat!

THE CLASSIC GAME FOR ALL AGES

FEATURING EXCITING NEW

**MEAT SPACE**

**THREATS!**

# Name That Threat!

It’s a worm

Discovered in 2008

Impacted British and French Naval systems

Led to formation of a large working group

# A. That Threat is:

CONFICKER

# Name That Threat!

Uses anti-debugging  techniques

Steals information from web forms

Advertised by author as:

“Professional shellcode-based bot”

# A. That Threat is:

Win32/Napolar

# Name That Threat!

May set off metal detectors at airports

1 in 10 of people at VB may be carriers

Causes toxic iron overloading

Can be fatal

# A. That Threat is:

Hemochromatosis

(HFE gene patent applied for in 1995, but not published until 1996)

# Name That Threat!

Used by Russians to attack Estonia

Often fatal

Mortality rate as high as 75% in places

# A. That Threat is:

Plague

(Plague infected bodies hurled into besieged city of Reval/Tallinn, 1710)

# Threats and Big Data Security

- Big Data Security = SIEM on steroids + supplements
- Real time analysis of all current and archived security information, events, management logs, including network activity at all layers of the stack, plus intelligence feeds, in order to:
- Flag anomalous behavior, identify threats, enable mitigation, improve protection, carry out forensics

# Big Data Security: the next big thing?

« BIG DATA

## BIG DATA TRANSFORMS SECURITY

Take an intelligence-driven approach to security management leveraging Big Data.

Learn more »

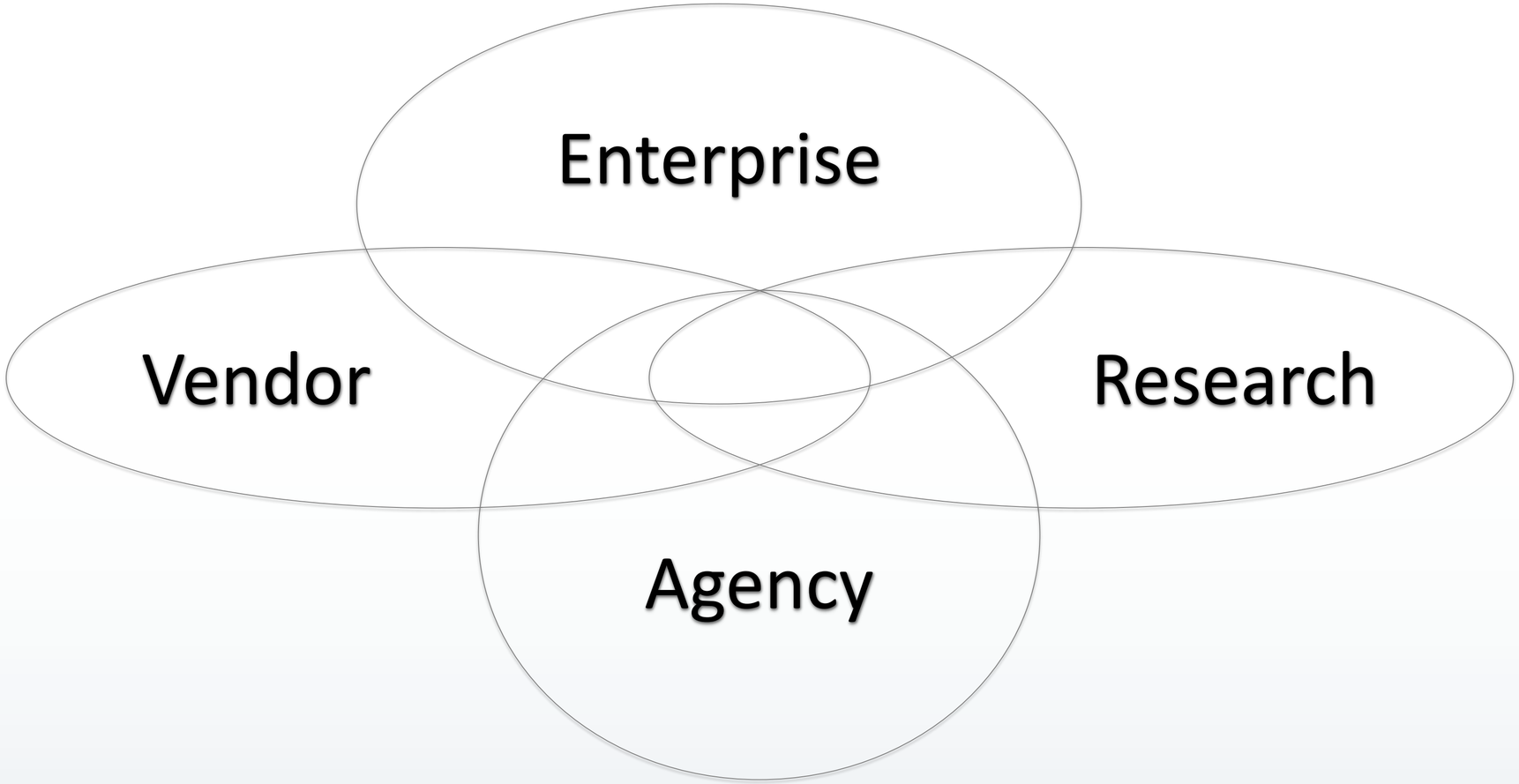
### How do you leverage Big Data to combat advanced threats?

Successful security management requires a system that extracts and presents security analytics quickly and effectively. RSA's intelligent, automated, and predictive approach helps security teams defend against modern threats—a constant race against time.

# Big Data Security and AV

- BDS marketing may add to the drumbeat:
  - Traditional antivirus is dead
- But good BDS will leverage AV threat data
  - If AV players participate
- Makes sense to play nice, and maybe lend a hand

# Big Data Security needs flows in/out



# Big Data Security needs sharing

- Anomalous network traffic
- Denial of service traffic
- Malicious code
- Malicious URLs
- Malicious email
- Zero days

# AV collaboration/sharing efforts

- NCSA 1988
- CARO 1990
- EICAR 1991
- Virus Bulletin 1989
- AVPD 1991
- WildList 1993
- Norman Sample Sharing Framework
- Conficker Working Group
- Wide array of ad hoc groups, lists
  - IEEE, invitation only, etc.
  - By threat family and threat elements
    - Spam, phishing, DDoS, malicious URLs, etc.

# Collaboration/sharing efforts

- More recent technical initiatives
  - MAPP, STIX, TAXII, MAEC
  - Real Time Threat List
    - Righard Zwienenberg, ESET; Richard Ford, FIT; Thomas Wegele, Avira
- Organizational and aspirational initiatives
  - NIST Cyber Security Framework (CSF)
  - IID: Sharing the Wealth, and the Burdens, of Threat Intelligence

# Lessons for Big Data Security

- From the Conficker Working Group and elsewhere
- Sharing requires trust
- Also takes people, resources, commitment
- Efforts must be orchestrated and organized
  - But tasking volunteers can be tough
- Standards of conduct must be agreed and adhered to
  - But wrangling volunteers can be tough
- Goals need to be defined

# Challenge for AV and BDS

- Obstacles include:
  - Politics
  - Profit
  - Vested interests
  - Egos
- Dimensions include:
  - Trans-national
  - Costly
  - Sustainability
  - End game

Some approaches are universally problematic…

# Bad choice #1: Owning threats

- Patenting the gene for hereditary hemochromatosis delayed diagnosis, treatment, research, cure
- Buying up zero days delays fixes, prolongs problems
- Not sharing samples hampers efficient detection
- Rewards for research? Yes
- Ransoming threat data? No

# Bad choices #2: Weaponizing threats

- Plague as a weapon did not end well, increased death toll throughout the region
- Malware as weapon reflects seriously flawed thinking particularly if adversary has/obtains good reversers
- AV industry must convince governments that deploying malware is simply a bad idea
  - Impossible to control or predict with any useful degree of certainty
  - Blowback and “back-at-you” are almost inevitable

# Good, bad or just ugly

- Government agencies could foster, facilitate, and drive threat sharing
- But there’s that history of sucking sounds
- And just as we were making progress
  - Along comes the surveillance state

NSA $10.8b

NRO $10.3b

# Recommendations for BDS

- Potential of Big Data Security will be limited if:
  - Threats are not shared beyond and between:
    - Enterprises, agencies, vendors, researchers
- The time to work on the threat sharing is now
  - Takes a lot more effort and resources than the marketing materials would seem to imply
  - Requires will and commitment
  - Plus trusted relationships and mutual respect
  - And a lot of education

# Questions!

- Visit www.WeLiveSecurity.com
- Email stephen.cobb@eset.com
- Twitter @zcobb
- Turn left for the bar