

Emerging Trends

Current State of Cyber Security

Dr. Eric Cole



How to **AVOID** becoming a statistic?

- PrivacyRights.org (updated weekly)
- Here are some that are reported (most are not)
- Just a small sample (financial records breached):
 - Heartland Payment Systems (130+ million – 1/2009)
 - Oklahoma Dept of Human Services (1 million – 4/2009)
 - International Finance Agency (22 million – 1/2010)
 - University of California (160,000 – 5/2009)
 - Network Solutions (5 million – 3/2010)
 - European Military Veterans Administration (76 million – 10/2009)
 - Australian BlueCross BlueShield Assn. (987,000 – 10/2009)

What are your executives most concerned about?

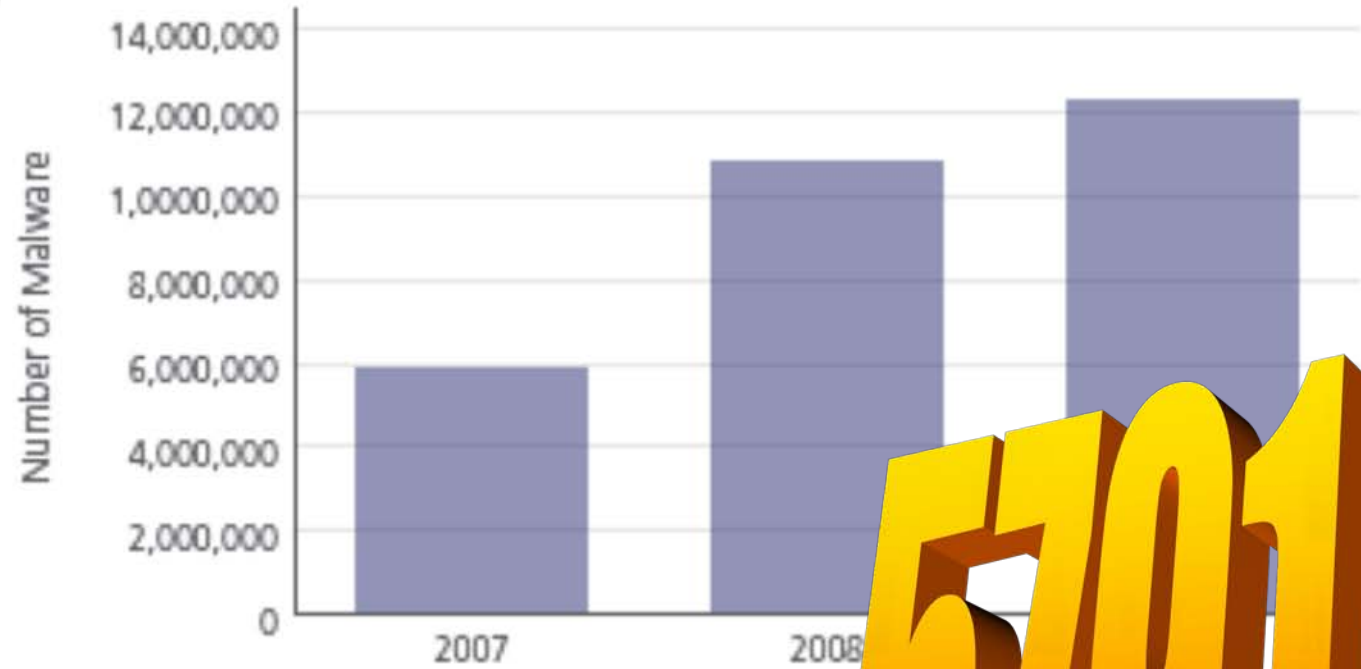


RON WHITE



*You Can't Fix
Steephead*

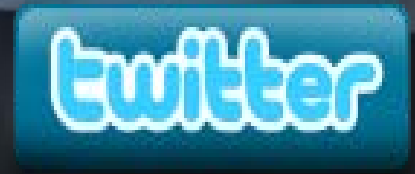
Data Driven Threats



5791 per day!

	1997	End of 2007	Mid 2010
Malware families	440	28,500	34,100
Password Stealers (Main variants)	400	80,000	380,000
Potentially Unwanted Programs	1	24,000	26,000
Malware (families) (DAT related)	17,000	358,000	484,000
Malware (main variants)	18,000 (?)	586,000	2,700,000
Malware Zoo (Collection)	30,000 (?)	5,800,000	16,300,000

Why Is This Happening? – Technology



What Is the Outlook?



Back to Basics

Offense

Defense

Likelihood

Impact

THREATS X VULNERABILITIES = RISK



Reduces Risk



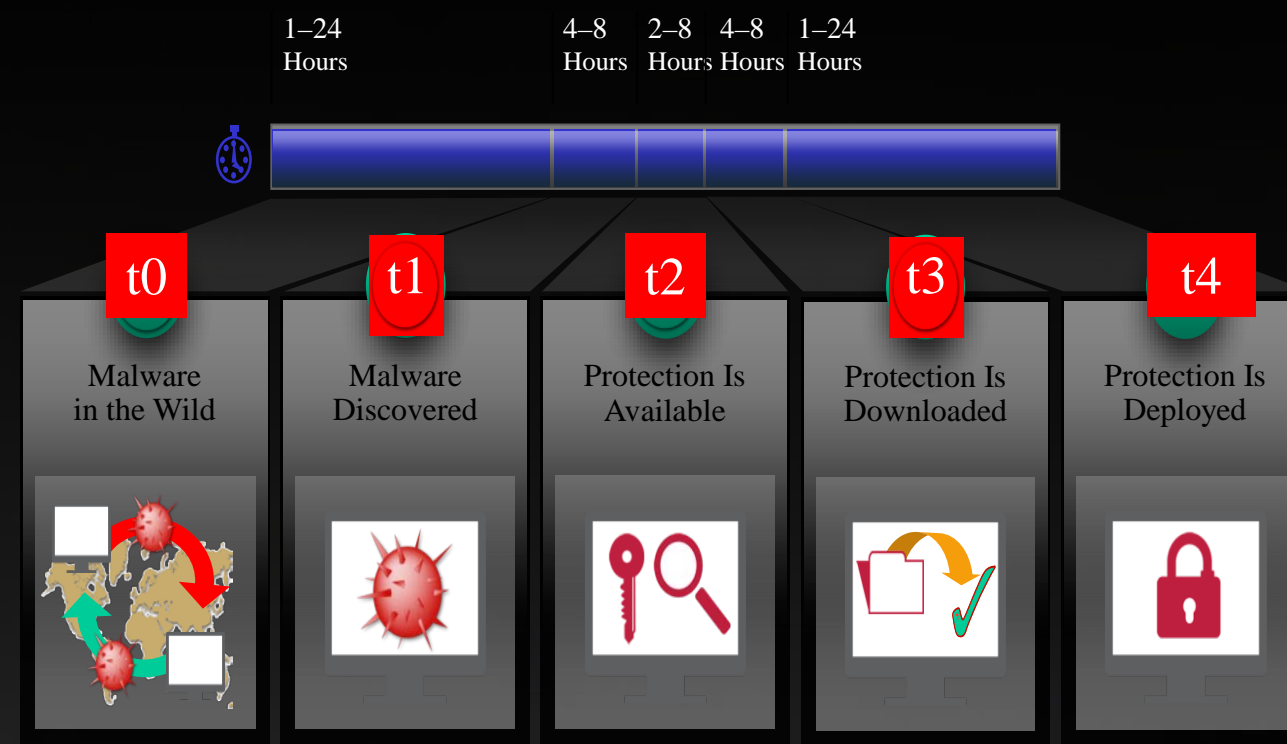
Drives risk calculation

However... **THREATS** Move at the

SPEED OF LIGHT



The **OLD** Model Is **BROKEN**



Protection Gap of
24-72 Hours

YES

<OR>

NO

REACTIVE

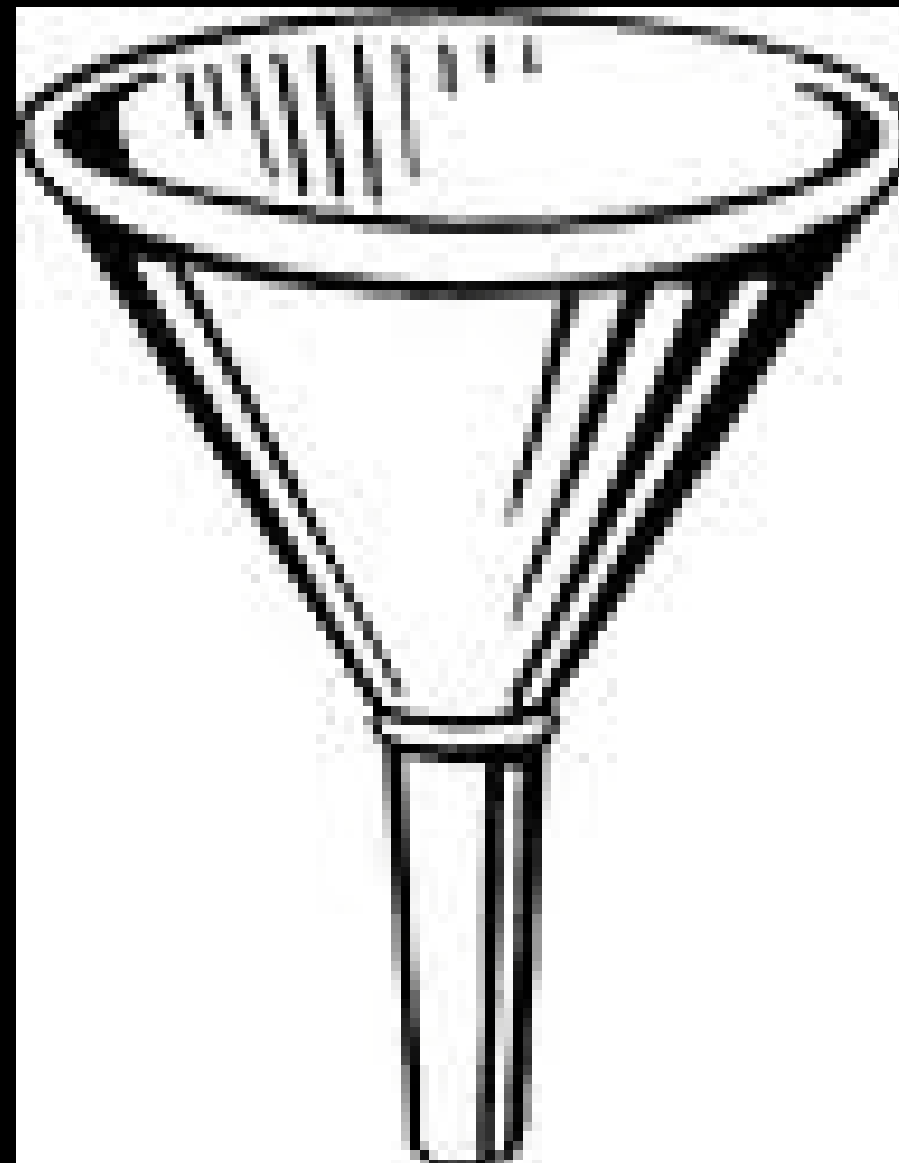
Current State of Security

- Attacks are increasing at an exponential rate
- This is contrary to what many people think because the attackers have changed how they operate
 - (Past) Visible → Stealthy (Today)
 - (Past) Disruptive → Data driven (Today)
 - (Past) Low hanging fruit → Targeted (Today)
 - (Past) Static → Dynamic (Today)
 - (Past) Ad hoc → Persistent (Today)
 - (Past) Basic → Advanced (Today)
- Many organizations are compromised for 6-9 months without detecting it
- Many organizations do not even realize they are compromised

2011 Emerging Trends

The background of the slide features a central bright white and yellow light source from which numerous thin, blue-tinted light rays radiate outwards in all directions. The rays are most concentrated in the center and become more sparse and dimmer as they extend towards the edges of the frame. The overall effect is one of dynamic energy and forward-looking technology.

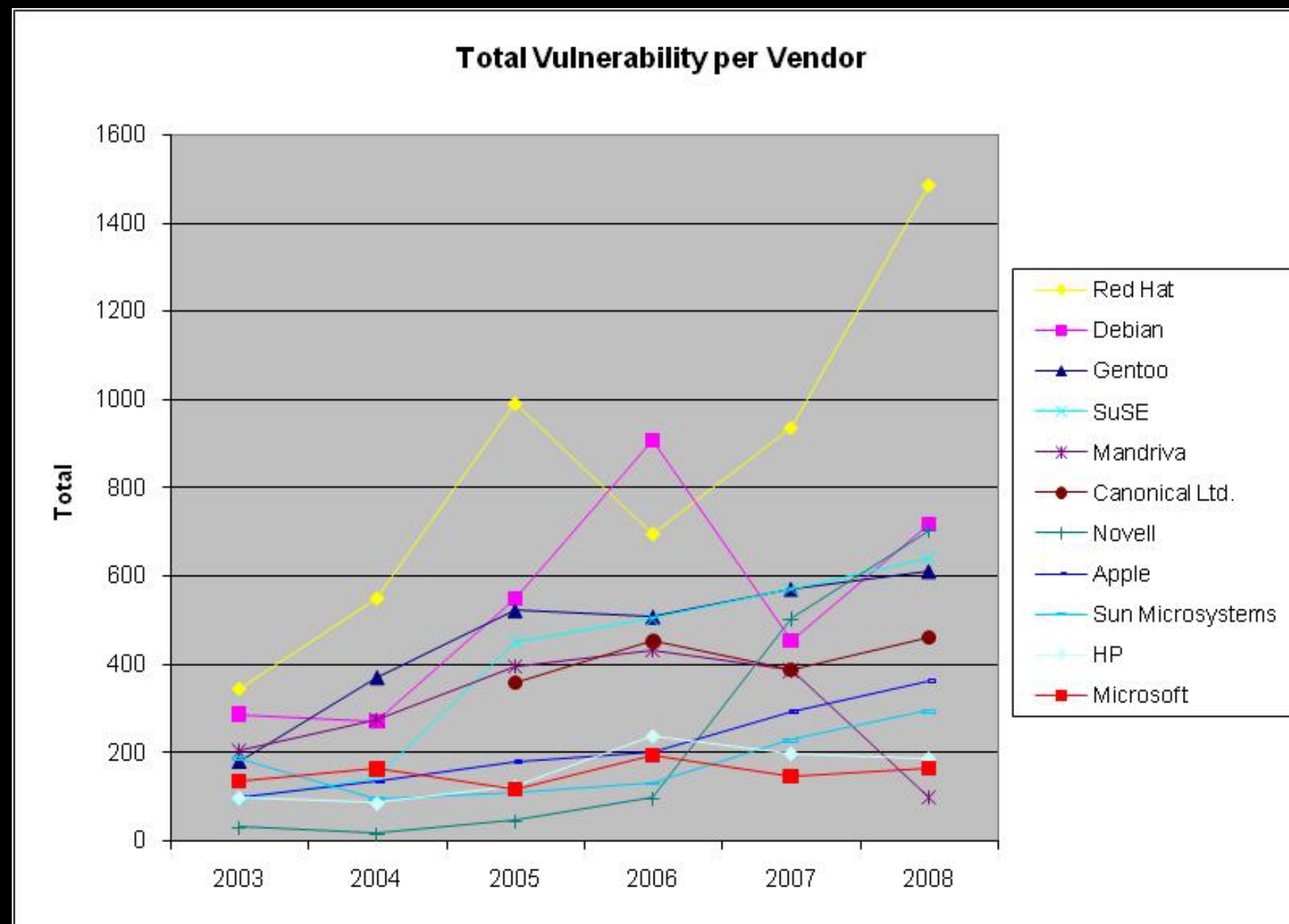
Trend 1: More focus on Data Correlation



Trend 2: Threat intelligence analysis will become more important



Trend 3: Endpoint security becomes foundation



Trend 4: Focusing in on proactive forensics instead of being reactive



Trend 5: Moving beyond signature detection



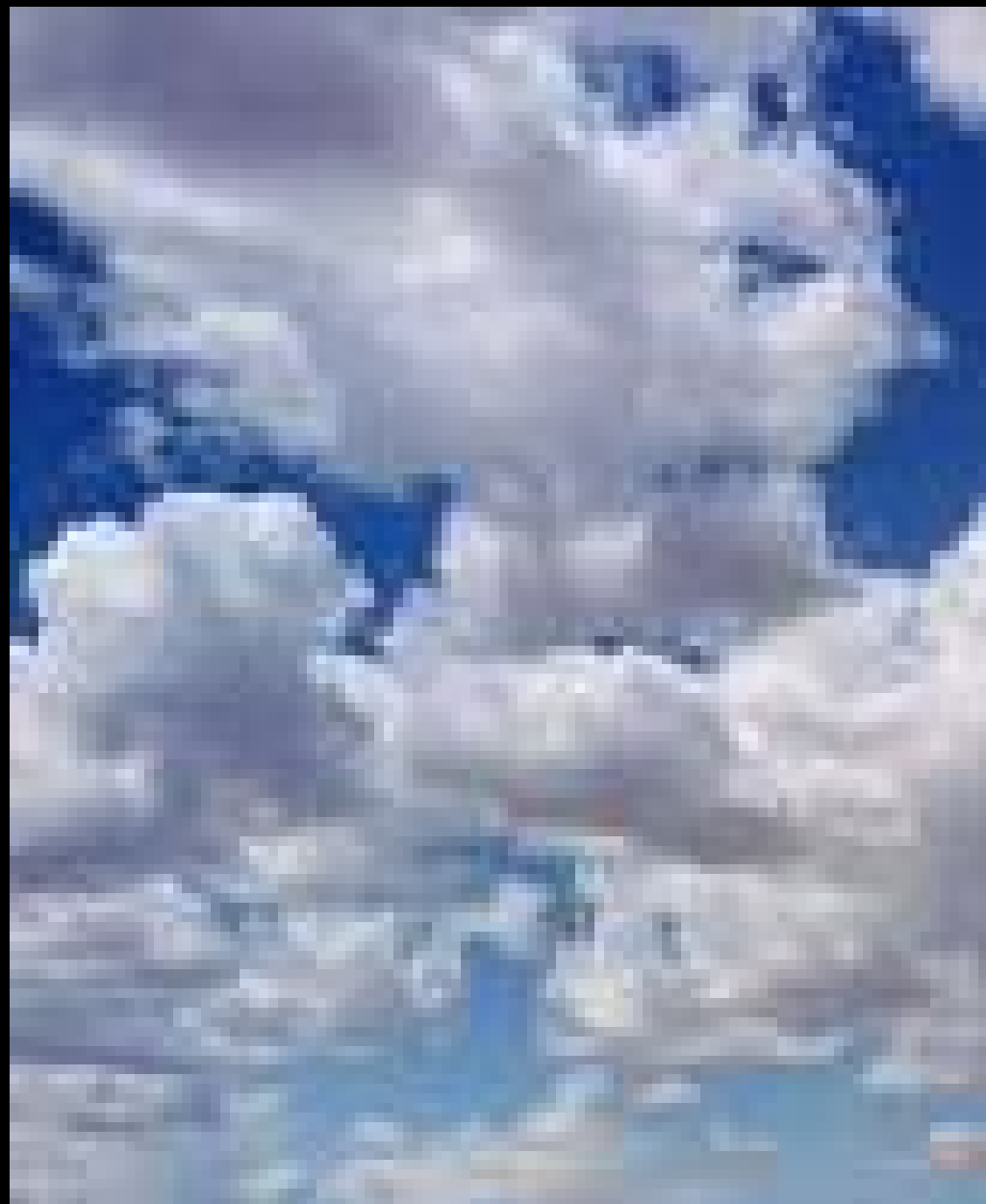
Trend 6: Users will continue to be the target of attack



Trend 7: Shifting from focusing on data encryption to key management



Trend 8: Cloud computing will
continue regardless of the
security concerns



The Future Is...

The image features a central, bright blue light source that radiates outwards, creating a tunnel-like effect. The light rays are composed of numerous thin, parallel lines that converge towards the center, giving a sense of depth and movement. The overall color palette is dominated by various shades of blue, from deep navy to bright cyan, set against a dark, almost black background. The text 'The Future Is...' is positioned at the top center in a clean, white, sans-serif font.

THE FUTURE IS...



YES

NO

PROACTIVE

THE FUTURE IS...



THANK YOU for your time

Dr. Eric Cole is an industry-recognized security expert with over 20 years of hands-on experience. Cole currently performs leading-edge security consulting and works in research and development to advance the state of the art in information systems security. Cole has experience in information technology with a focus on perimeter defense, secure network design, vulnerability discovery, penetration testing, and intrusion detection systems. Cole has a master's degree in computer science from NYIT and a PhD from Pace University with a concentration in information security. Dr. Cole is the author of several books, including *Hackers Beware*, *Hiding in Plain Site*, *Network Security Bible*, and *Insider Threat*. He is the inventor of over 20 patents and is a researcher, writer, and speaker. He is also a member of the Commission on Cyber Security for the 44th President and several executive advisory boards. Dr. Cole is founder of Secure Anchor Consulting in which he provides state of the art security services and expert witness work. Cole is actively involved with the SANS Technology Institute (STI) and SANS working with students, teaching, and maintaining and developing courseware. He is a SANS faculty fellow and course author.

Dr. Eric Cole



Twitter: [drericcole](#)
ecole@secureanchor.com
eric@sans.org