INTERNET SECURITY ALLIANCE

AEROSPACE INDUSTRIES ASSOCIATION

Sponsored by Raytheon

Customer Success Is Our Mission

Aero Webinar Series

An Information Assurance Strategy for the Rest of Us

Jeff Brown
CISO
22 October, 2009

Copyright © 2009 Raytheon Company. All rights reserved.
Customer Success Is Our Mission is a registered trademark of Raytheon Company.

Upcoming AIA/ISA Webinars

- **Testing In A "Real" Environment Leads to Faster Cyber Security Innovation** featuring General (Ret.) Charles "Charlie" Croom, Vice President of Cyber Security Solutions, Lockheed Martin Information Systems & Global Services and Curt Aubley, Chief Technology Officer CTO, Lockheed Martin Operations & Next Generation Solutions. To be presented on 11/5/09
- **Supply Chain Issues in Cyber Security — A Framework for Moving Forward** featuring Scott Borg, Director and Chief Economist (CEO) at the U.S. Cyberconsequences Unit. To be presented on 11/19/09
- **Legal Framework for Securing Unified Communications** featuring Jeffrey Ritter, President, Waters Edge Consulting.

Raytheon

Roadmap

The Advanced Persistent Threat

- Increasingly sophisticated cyber threats by hostile entities designed to gain control of your network for the long term
- Intellectual property theft on a grand scale
- Not just one particular country or group
- Aerospace companies are target #1!

TIME Partners with CNN

U.S. ADD TIME NEWS

INSIDE: Main | The Page | Politics | Swampland | Real Clear Politics | Whi

The Invasion of the Chinese Cyberspies (And the Man Who Tried to Stop Them)

The Washington Times

US News | National Security | Just the Headlines | Front Page Image |

Home | News | Voices | Sports | Culture | Th

World | National | DC Area | Politics | National Security | Business | Entertai

Chinese hackers prompt Navy college site closure

Originally published 10:30 a.m., November 30, 2006, updated 12:00 a.m., November 30, 2006

Chicago Tribune

chicagotribune.com

Archives National

You are here: Chicago Tribune > Archives > 2008 > November > 30 > National

Archive for Sunday, November 30, 2008

Cyber attack has Pentagon worried

Russia eyed in hit on Defense networks

Raytheon

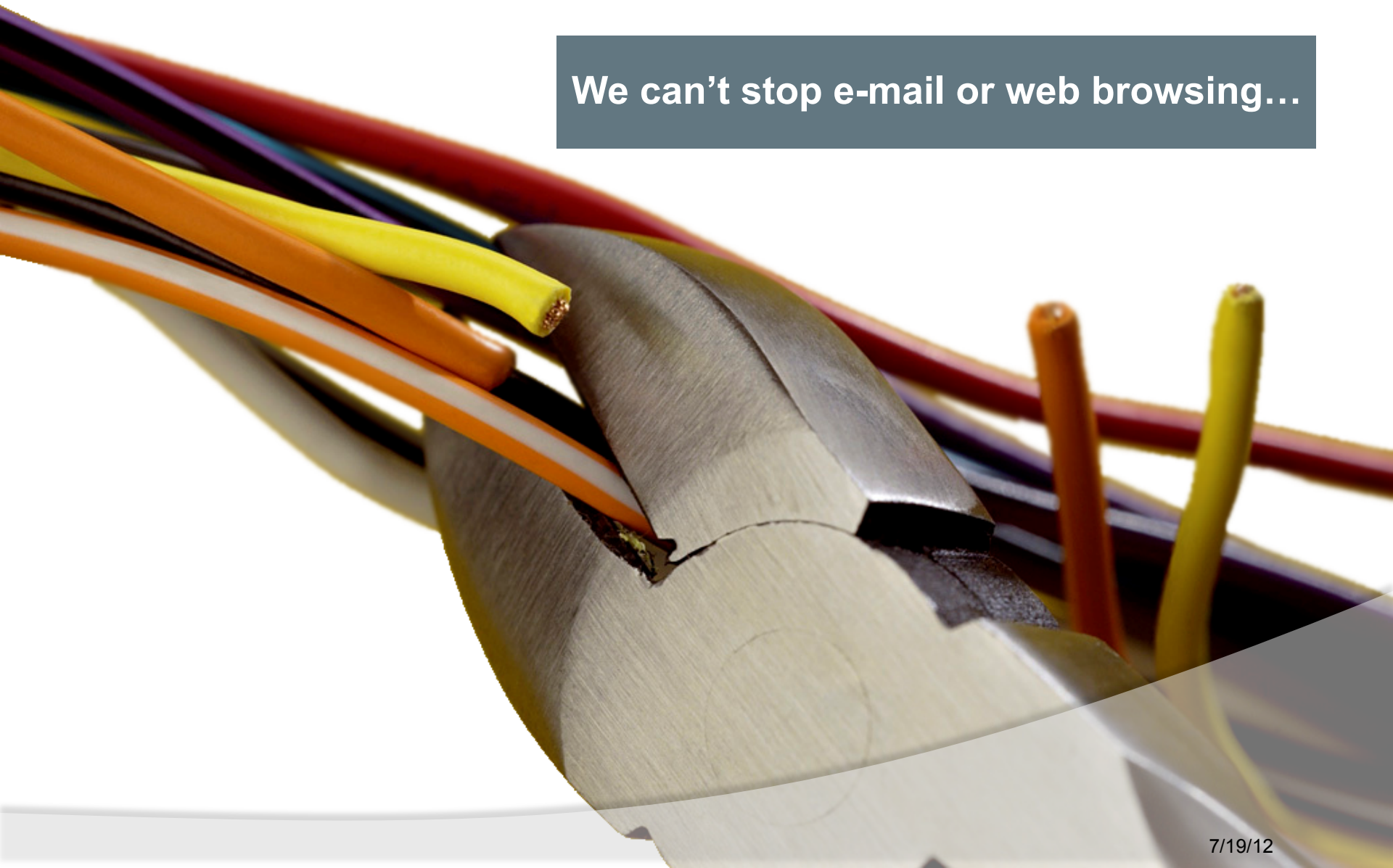
None of us – big or small – can stop a determined cyber attack from succeeding!

We can't rely on traditional defenses (good patching, firewalls, IDS, AV, etc.) in the age of social engineering and zero-day exploits

- But how much can you invest in cyber security?
- Likely not a fraction of what DoD and the Big Primes are investing.

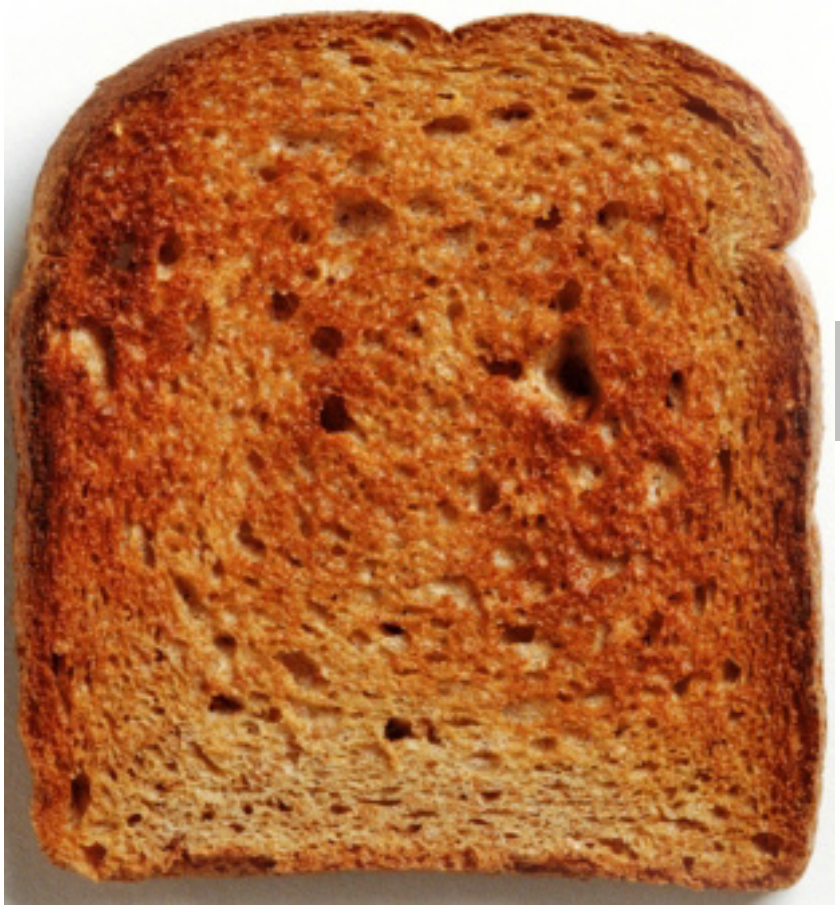
Raytheon

So Where does that leave us?



We can’t stop e-mail or web browsing…

It would be easy to be pessimistic



But you'd be wrong…

There is a strategy that can give you a lot of lift

Raytheon

A Strategy for the Rest of Us

- Recognize they will get in.
- Work to detect and disrupt outbound command and control channels.

If intruders get in, but can't get back out, we win!

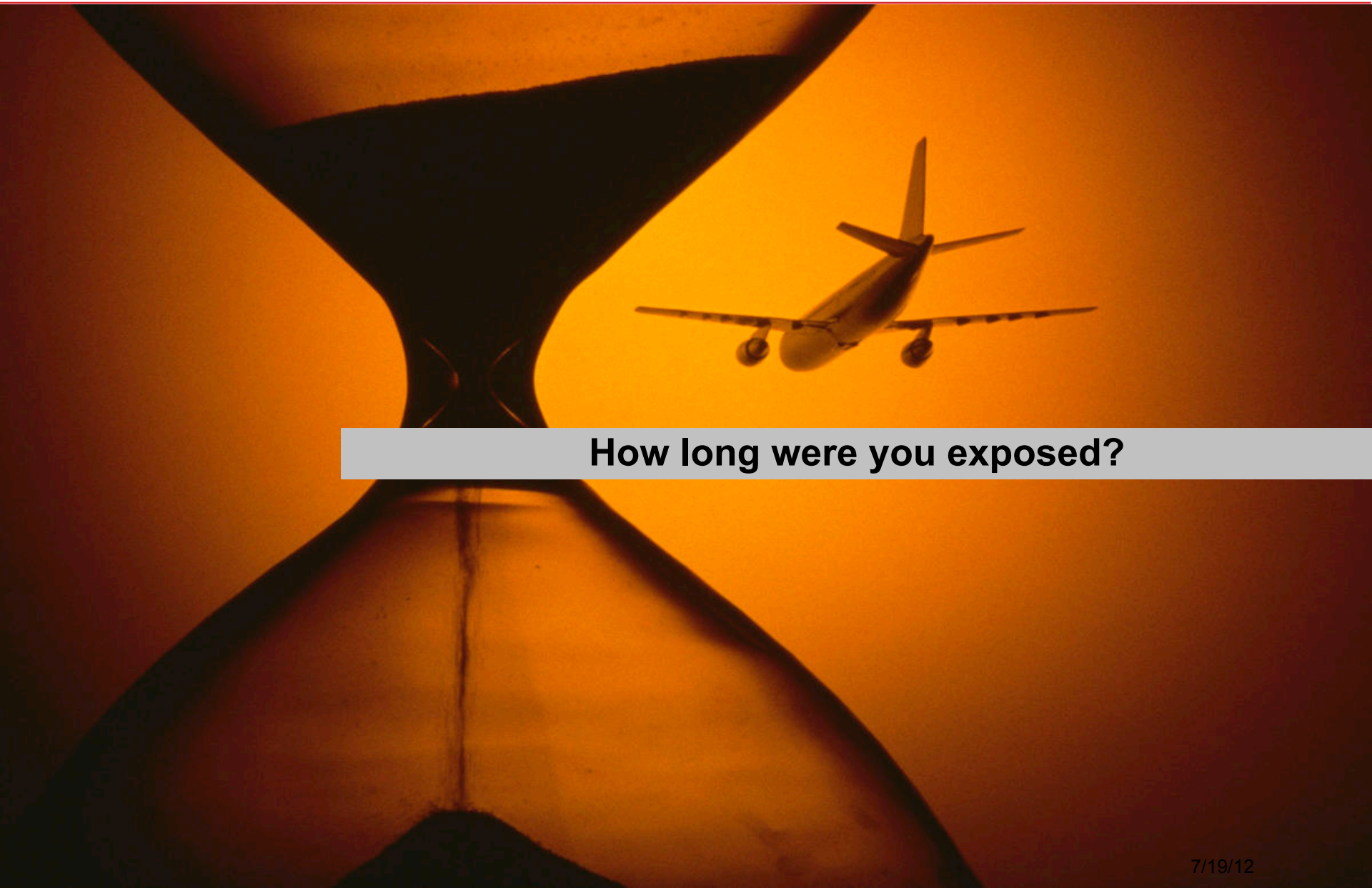
If your infrastructure addresses the fact that intruders will get in, the number of intrusions becomes much less relevant.

Which has less risk?

- If 100 get in and can't get out or only last a day before C2 monitoring finds them
- If 10 get in and have free reign for 3 months before a sys admin finds them

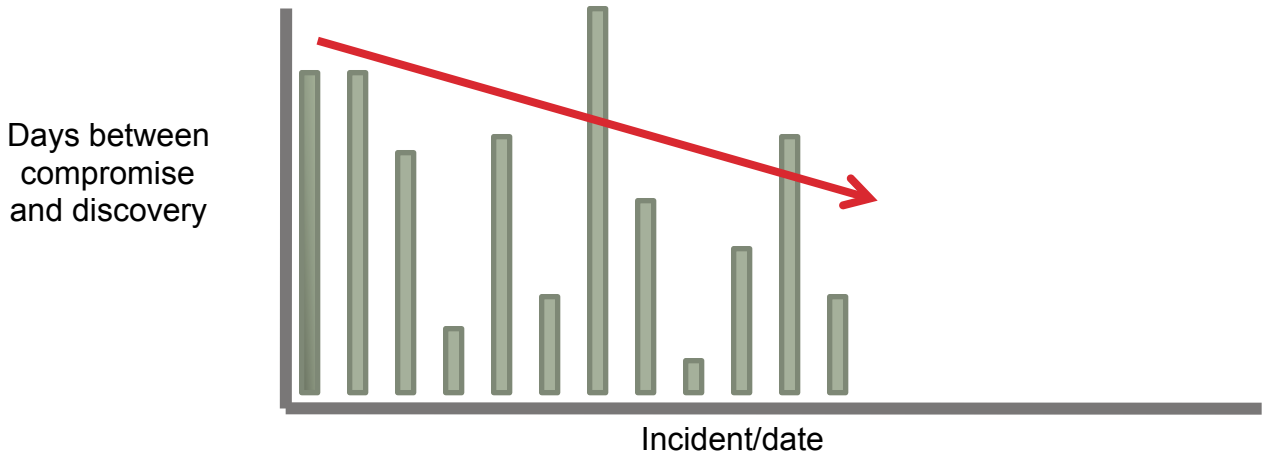
The Primary metric becomes "Dwell Time"

Raytheon



Your Goal

- **Your goal should be to drive down Dwell Time anyway you can.**
- **If Dwell Time trends down, your cyber security is improving**



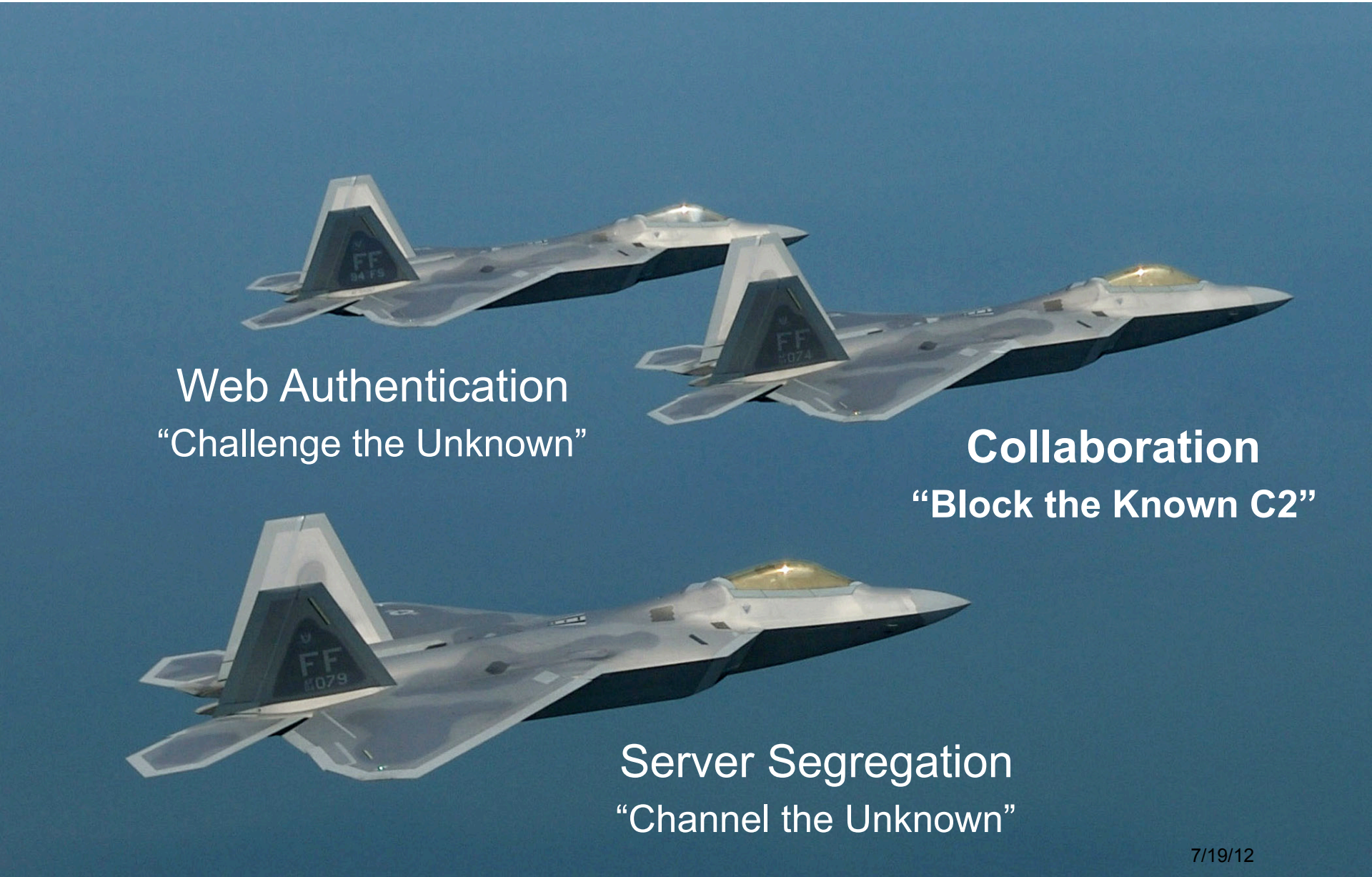
Raytheon

So Focus on Outbound Traffic

- It's easier and the highest payoff!
- There is far less noise on outbound traffic
- It decouples malware detection from the vulnerability

Disrupt and Deny Adversary's Command and Control Traffic

3 Ways to Make This Strategy Real



Web Authentication

"Challenge the Unknown"

Collaboration

"Block the Known C2"

Server Segregation

"Channel the Unknown"

Blocking the Known

Raytheon

Discover and block C2 sites any way you can

Collaboration is Cheap.

You can use other people's money!

The Return on Investment is high

The Value of Collaboration

The Hard Way:

Go it alone. Invest heavily. Find one C2 site for every compromise. Find it through good sys admins, dumb luck, or “the phone call”

The Easy Way:

500 companies find one C2 site each the hard way.
You get 499 for free.

Raytheon

You Don't Have to Share Much

We saw malware beaconing or communicating to www. badsite.org or 123.45.67.211

- You're not admitting you were compromised, just that you found something

Share the outbound traffic info!

Raytheon

Collaboration Opportunities

- ISACS
- Defense Industry Base Cyber Task Force
- Law Enforcement (Infragard)
- Defense Security Information Exchange
- Amongst Yourselves

Measure of Merit: is it near-real time?

Raytheon

3 Ways to Make This Strategy Real

Web Authentication

"Challenge the Unknown"

Collaboration

"Block the known C2"

Server Segregation

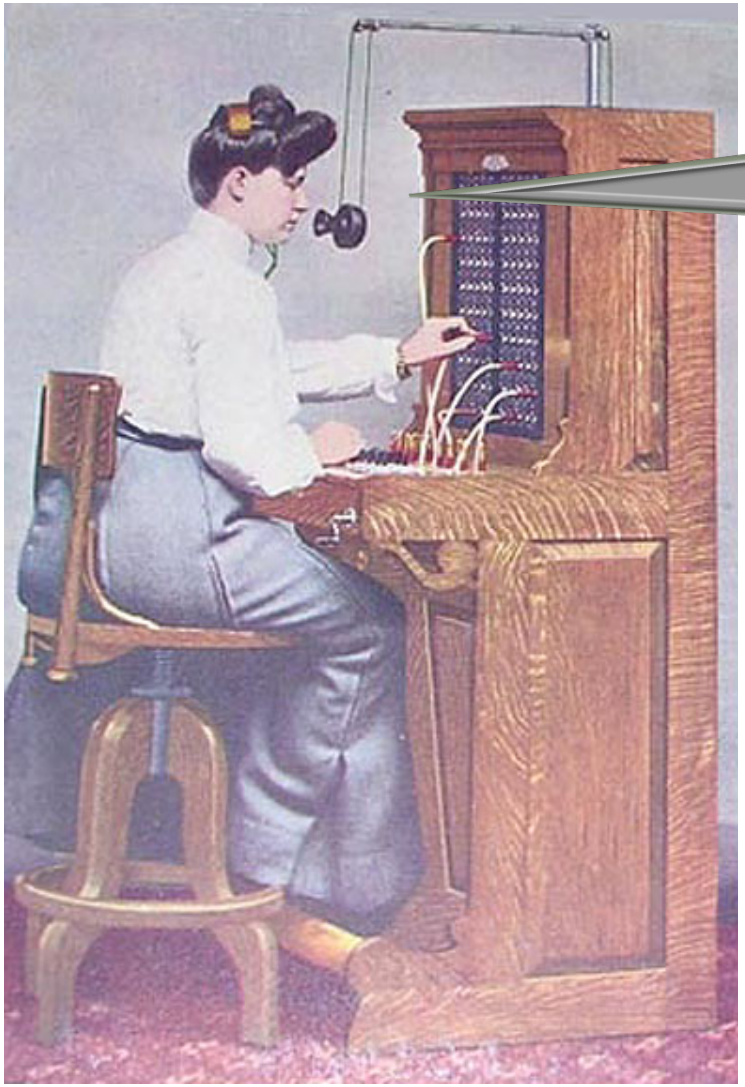
"Channel the Unknown"

Raytheon

Servers - “It’s where the money is”

- Servers are where the adversary wants to live
  - On 24x7
  - Contains the most valuable data
- Limit unknown traffic to and from them

Channeling the Unknown



I'm sorry, file server, I can't connect you with www.badguy.com

- Most servers have no business initiating traffic to the Internet except for very specific sites (Updates, etc.)
- It is easy to enumerate valid destinations

Channel all Server Traffic

- Servers should only talk to the Internet through known choke point to known sites
  - Put them in a separate subnet(s)
  - Point all to a separate proxy
  - Permit only mission essential sites
    - Proxy denies become meaningful
    - Allow sys admin 2-factor authentication overrides
  - Above all, prohibit sys admin e-mail and surfing

Raytheon

What Does That Do For You?

- No way for malware to beacon to owner
- To access a server, they must compromise a client and move laterally
  - Much noisier
  - Combine with two factor authentication for servers and you really have something
- **Experience shows that all malicious traffic moves to clients overnight**
  - And it cost nothing except the labor to consolidate server subnets and identify valid sites

Raytheon

3 Ways to Make This Strategy Real

Web Authentication

"Challenge the Unknown"

Collaboration

"Block the known C2"

Server Segregation

"Channel the Unknown"

Challenge the Unknown

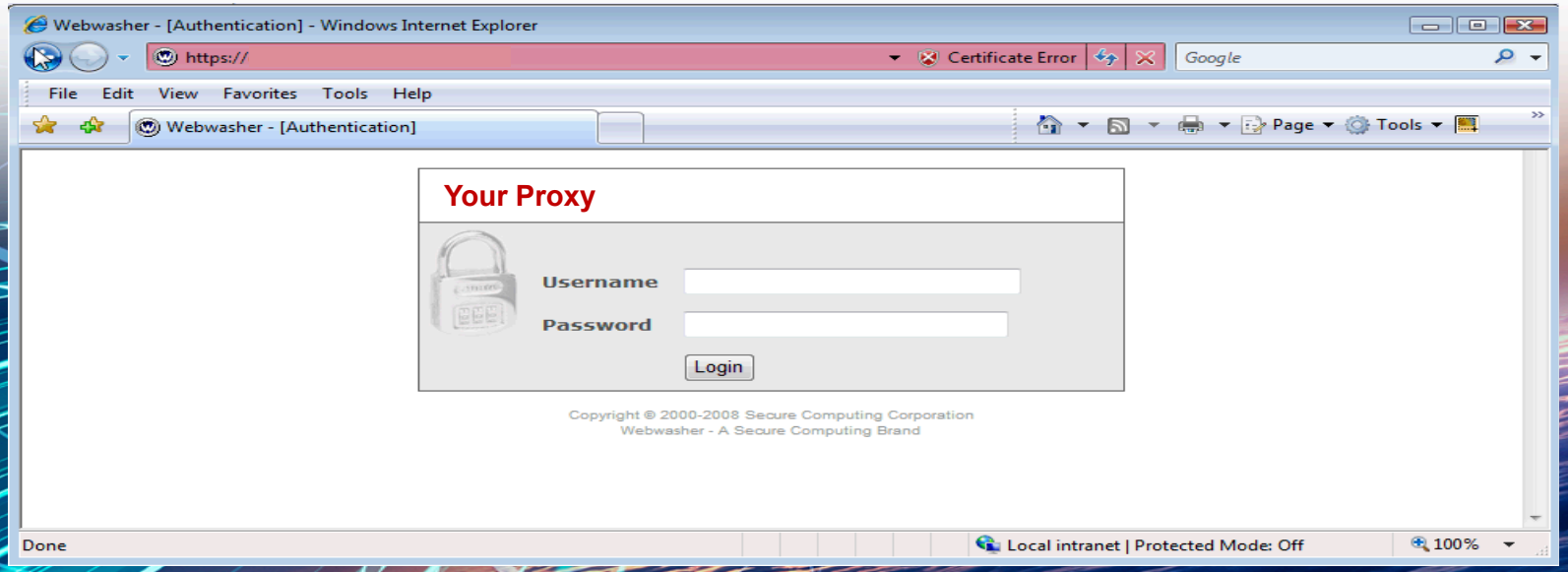
- All web proxy vendors "categorize" sites and update like AV
- The majority of malware C2 sites are new and therefore fall into the default "uncategorized" bin
- This presents us with an opportunity

You want to go where?!!!

Raytheon

Even a Small Speed Bump is Effective

- Most malware can't deal with a graphical input request
  - Demand adversary do a lot more work to succeed
- Authentication denies may highlight compromises
- Users can still go where they want to go
  - You have an audit trail
  - This may server as a deterrent for non-business related activity



The Bottom Line – Don't Despair

By adding a C2 Denial Strategy to your existing Defense in Depth you can improve your cyber security greatly without breaking the bank

Set yourselves up for success

Questions?