RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Cybersecurity the Old Fashioned Way: Pass Known Good

SESSION ID: : HT-W03

Moderator: Dr. Peter Fonash
CTO DHS/NPPD/CS&C
Peter.Fonash@DHS.gov

Panelists: Dr. Brian Done
Cyber Architect
DHS/NPPD/CS&C

Boyd Fletcher
Technical Director
NSA/I223

Tom Ruoff
Program Analyst
DHS/NPPD/CS&C

Ann Barron-DiCamillo
Director, US-CERT
DHS/NPPD/CS&C

Problem we are trying to solve

Detection and protection from zero day malware in a way that is:

- Low/moderate cost per user
- Scalable to Federal Executive Branch and Critical Infrastructure, then every one else
- Thoroughness; covers the protected domains with no back doors
- Effective; provides significant improvement over current capabilities
- Complete; stop bad but pass good

Why Current Approach is not Working

- A/V and Hash Clouds
  - Completely ineffective against zero day threats; need a prori knowledge and rapid dissemination of information (signatures)
  - Multiple industry reports show A/V is trending towards increasing ineffectiveness
- Detonation Chambers
  - Effective in detecting some zero days but malware authors getting better in countering capability
  - Does not address data exfiltration

Is There Another Way?

Yes, pass known good

- Most common technique is deep content inspection and sanitization
- Relies on in-depth understanding of file types and protocols
- Not signature based
- Writes out known good content
- Removes content that does not fit protocol or is not structurally correct
- Most malware is very fragile, cannot survive transliteration changes

Questions and Panel Discussion

BACKUP SLIDES

How to Transform Content and Pass Known Good

How do you pass "known good" – the four techniques.

1. Deep Content Inspection and Sanitization: verify object type/protocol, contents and only writing out known good content
2. Format Conversion: transform content into a format that retains information but is inspectable (PDF to PS to PDF)
3. File Flattening: Convert complex file to simple file formal to remediate vulnerabilities in complex protocols
4. Canonicalization: Normalization, convert contents from specialized into normal or standard form, audio files into PCM

How well does it work?

Review of Testing

- AFT blocked or sanitized 99% zero day malicious content – no a priori knowledge of malware
- Passed 98.5% of known good content
- Goal of development effort is 99.9% pass known good

TERMS: The cross domain solution inspection engine is called Assured File Transfer (AFT). The email instantiation is eMIST and uses the AFT engine.

What is our answer?

"Pass Known Good"

HOW?

Transform content from format capable of housing bad content to one that does not enable or allow for bad content to be active, using existing cross domain solution (CDS) filtering technology

Example: In graphic files, introduce noise to a level that is not human detectable but that fractures coherence of malware instructions

Our Answer – Part 2

Where do we get this capability?

- The US Dept of Defense has been developing systems that do this type of information processing in the Cross Domain Solutions (CDS) area.
- The CDS engine that specializes in the area is called Assured File Transfer (AFT): AFT cleaning USB devices is FIST, AFT inspecting email is eMIST used for 3 years at DISA to pass email between NIPRNet/SIPRNet (1.1M processor hours in load balanced system).

Why is this innovative and new?

Because the CDS and protection communities don't interact so much…lateral application of TRL 8 systems to different problem space

How well does it work?

Review of Testing

- NSA/ISIS contract took SEI malware samples and ran on larger processor, same AFT 1.3.1 policy
- The 38,191 files expanded to 493,313 objects processed (embedded objects)
- 17,080 files sanitized (passed to output device) - 21, 108 files blocked
- AV testing showed 170 of passed files activated multiple AV engines (47 used)
- 170/38,191 = .0045 or 0.5% malware **may** have passed

Where is DHS Going With Content Filtering?

Current Programmatic Activities

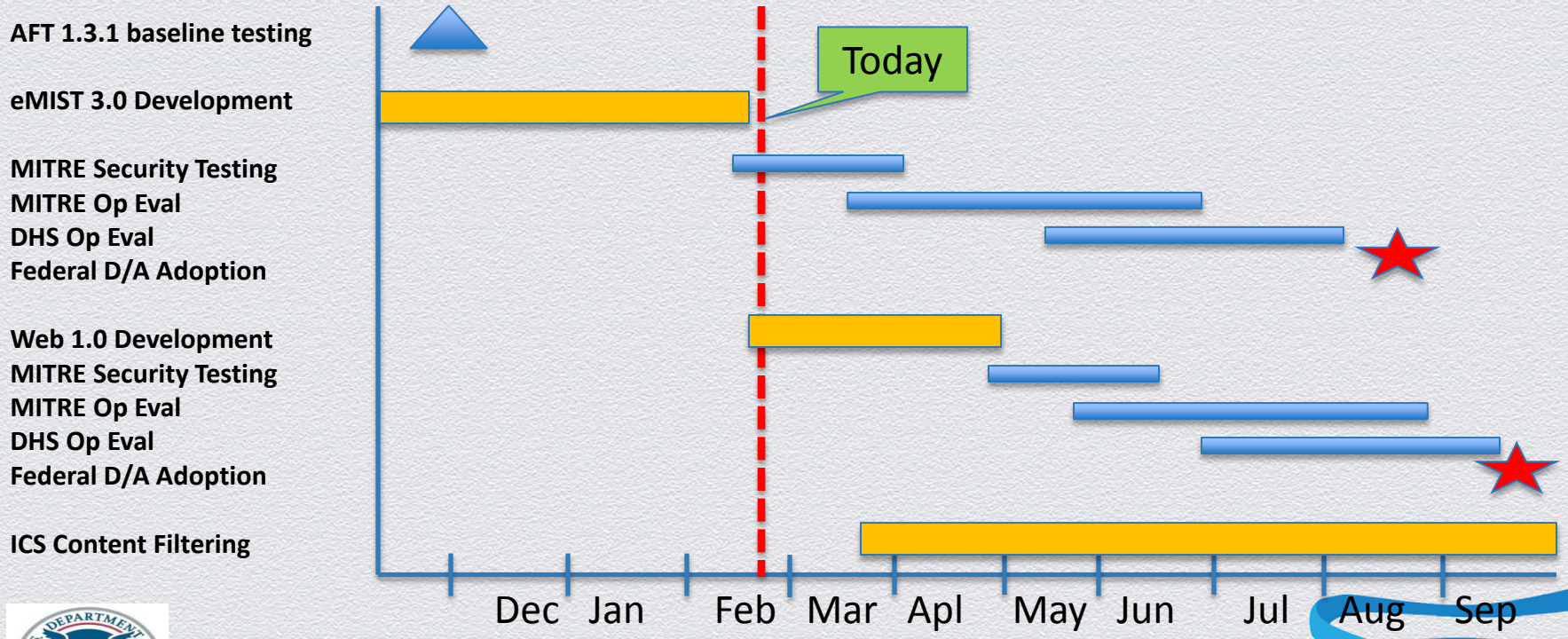
- Building eMIST 3.0: AFT for email
  - Email sanitization for Federal Executive Depts and Agencies/Critical Infrastructure sites at boundary
  - Aid in recovery from attack (stop bleeding)
  - Clean hosts: download files from compromised computers and save only “known good” for re-constituted systems
- Operational Evaluations at DHS and MITRE for enterprise email content filtering

Where is DHS Going With Content Filtering?

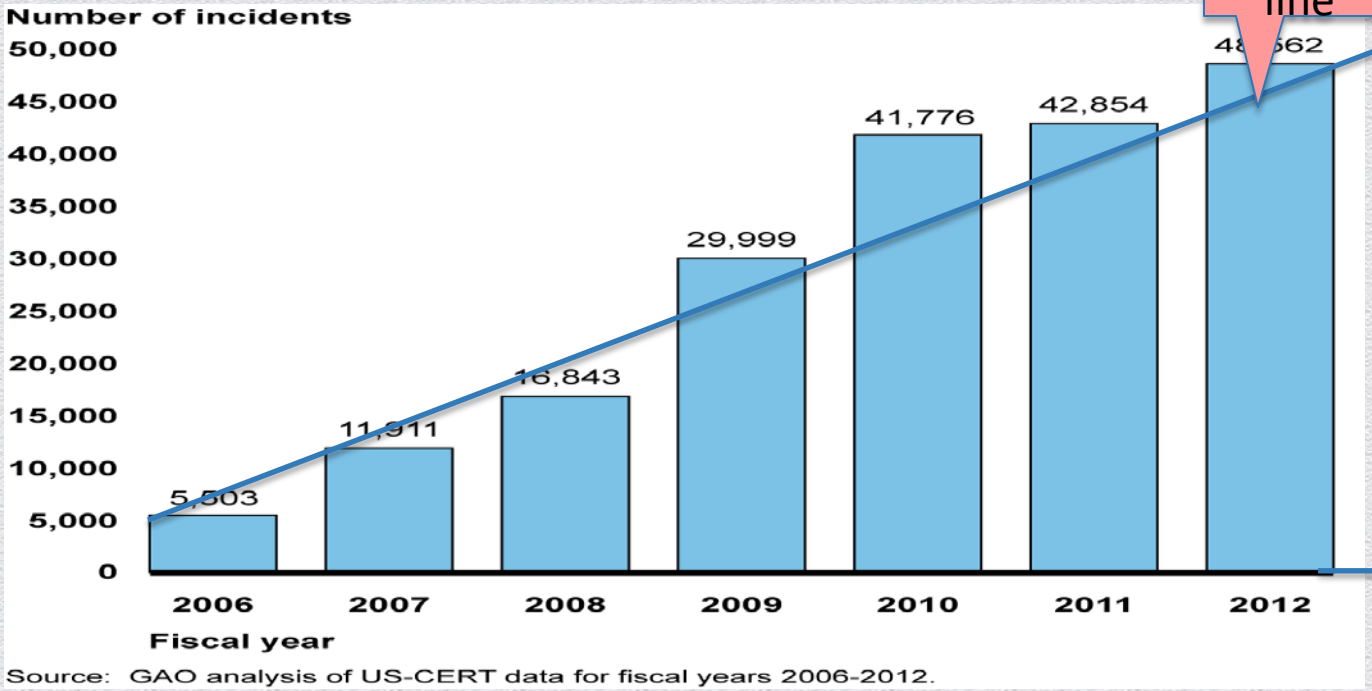
Future Programmatic Activities

- Build Web 1.0: AFT for web traffic
  - Integrate AFT as a side car with Squid web proxy
  - In-line device to sanitize/block malware
  - Conduct security/operational testing at MITRE/DHS
- Build Industrial Control Systems (ICS) content filtering devices for critical infrastructure processes filtering
  - inspect message format and set points

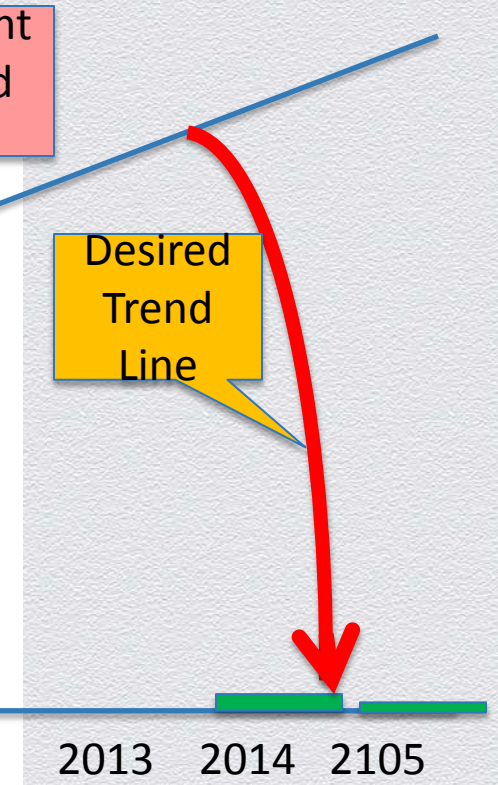
DHS Content Filtering Activities



Measurement of Success



Source: GAO analysis of US-CERT data for fiscal years 2006-2012.



What is the capability gap today in malware protection we are trying to solve

Most everyone is using the approach of trying to detect “known bad content”: results are steady increase in incidents…Exceptions are detonation chambers and statistical anomaly systems

We need a means to protect against email and web spread malware that is much, much better than signature based systems at same or less cost that can:

- protecting against **all** threats
- timeliness of providing protection once anomalous behavior is detected traffic
- Scalability – 250,000 users per domain
- Adaptability of bad actors to “trick” solutions

Why Do We Care About Capability Gap?

Current Methods are not working

If you experienced flat tires at an increasing rate, you'd change something….the increase in cybersecurity compromises indicates a need to seek alternative approaches – see next slide

How are we doing business today?

Block or Detect Known Bad

Blocking known bad assumes a priori knowledge of characteristics of bad content (signatures). Issues include zero day and time lag in distributing signatures

OR

Detecting or recognizing bad behavior assumes the bad content will present readily (timeliness)

These are all good techniques but leave room for in-depth mitigation enhancements

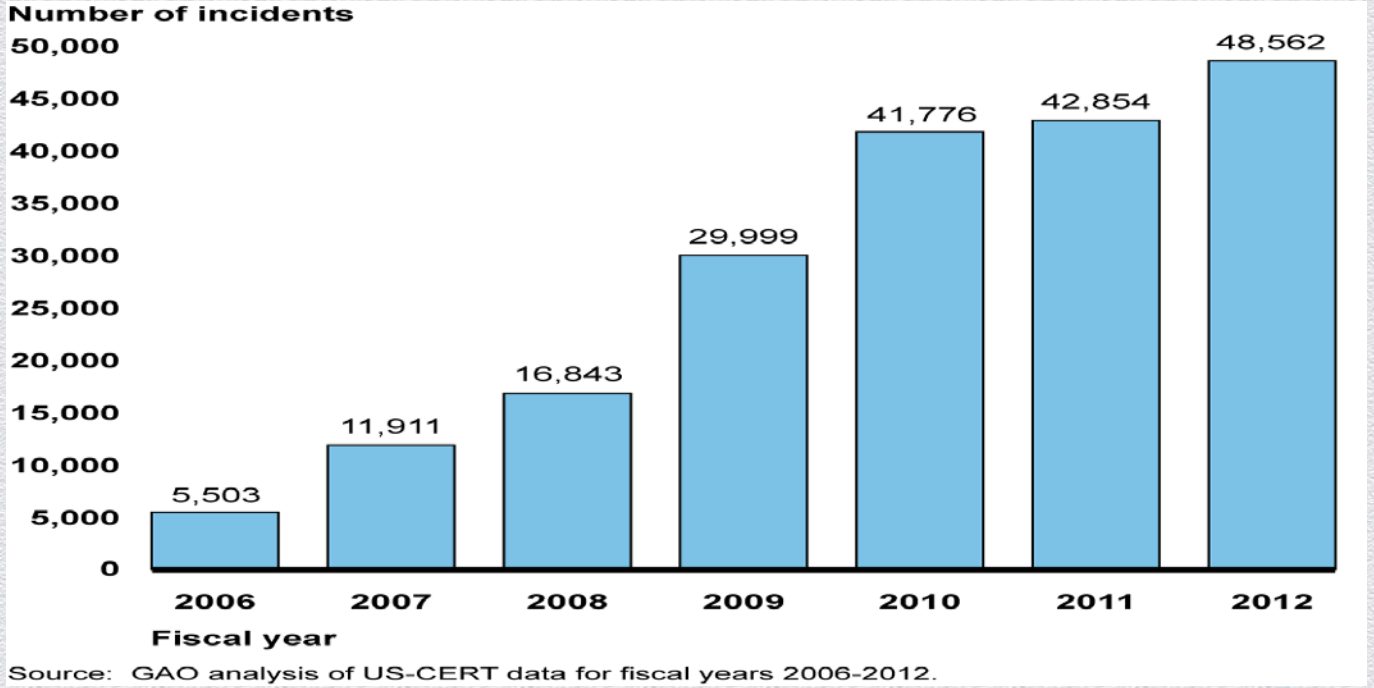
Why Do We Care About Capability Gap?

Loss of US IP:

- The annual losses are likely to be comparable to the current annual level of U.S. exports to Asia—over $300 billion.
- Loss of Millions of US Jobs
- Drag on US GDP Growth
- Diminished Innovation

(REF IP Commission Report 052213)

Motivation to Seek New Cybersecurity Methods



Source: GAO analysis of US-CERT data for fiscal years 2006-2012.

Where is DHS Going With Content Filtering?

Desired End State

“Significantly enhance cybersecurity posture for Federal Executive Branch Departments and Agencies as well as critical infrastructure owners and operators Information Technology systems through use of commercially available cross domain solutions technology applied at the enterprise level, acquired individually by each entity at market driven cost.”

How well does it work?

Review of Testing

- SEI was sent a version of AFT
  - Around 10,000 files with documented malware processed and passed to output device
  - Output was sent thru AV scanning, 84 samples activated some AV engine

    (84/10,000 = 0.0084)
- MITRE sent 24 CVEs in 47 files thru their AFT 1.3.1
  - 45 of 47 malicious files were blocked or cleaned
  - 2 of 24 CVEs activated their AV after filtering, these 2 were partially cleaned – implant was removed but file tripped in sandbox
  - Inconclusive if malware was intact since combustion engine did not detect