Surviving 0-days

reducing the window of exposure

Andreas Lindh, VB2013

iSECURE

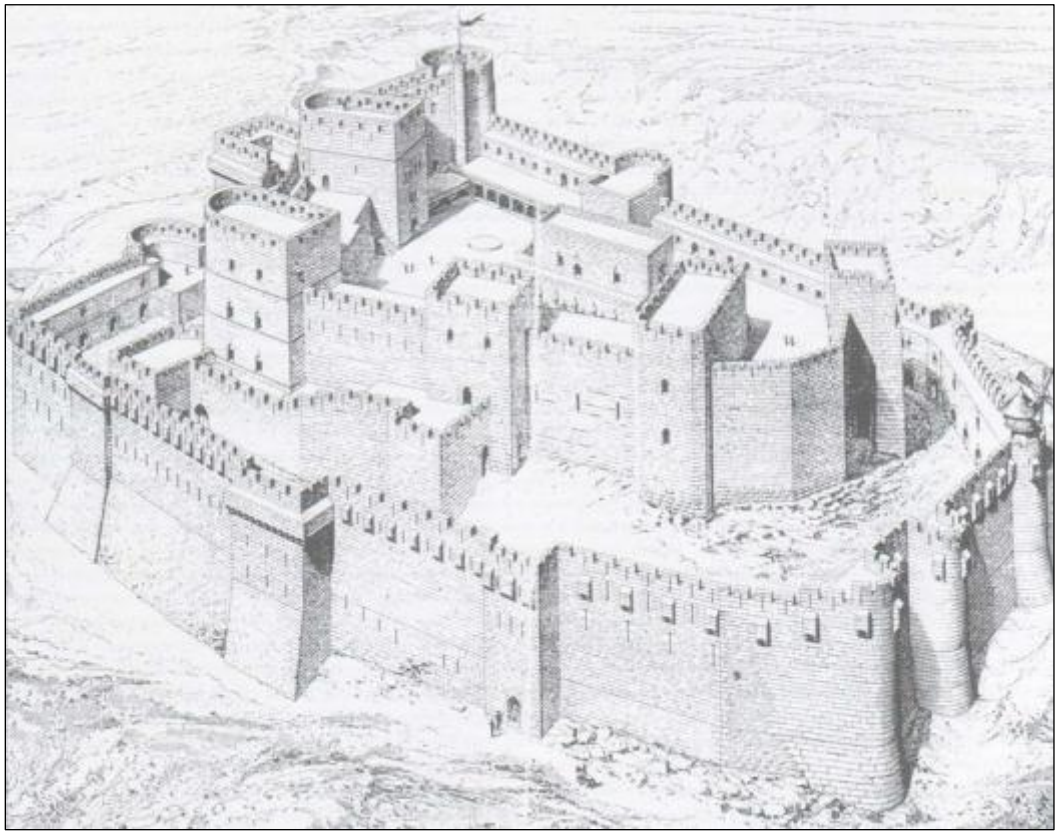
About me

- Security analyst/architect
- Used to work for Volvo IT
- Defender by profession
- @addelindh on Twitter

So what's this about?

- Software vulnerabilities, exploits and the current defense model
- A suggested way of improving that model

Defense



Legacy implementation

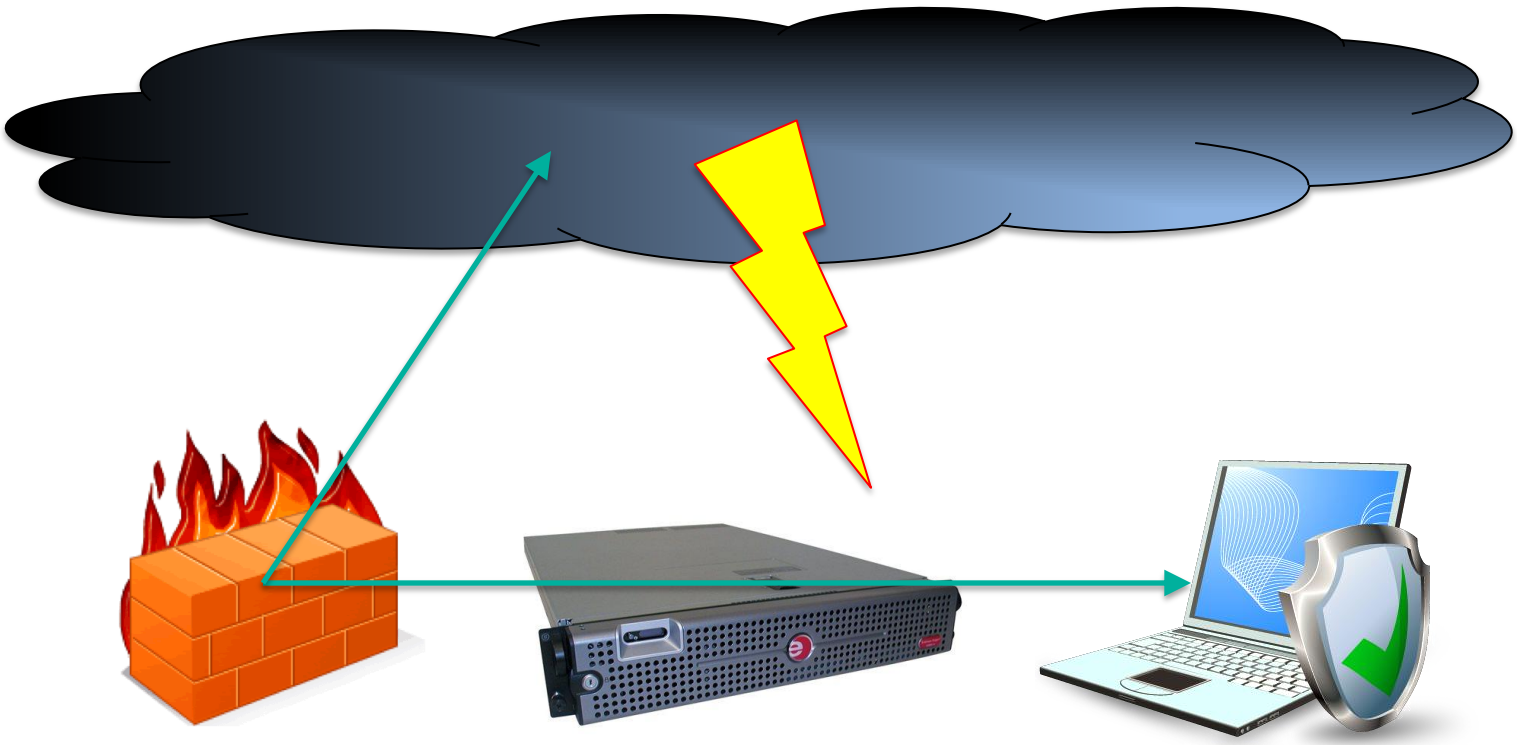
- Perimeter protection
- Access controls
- System hardening
- Antivirus

Evolution

- All the legacy and more:
  - SIEM
  - DLP
  - Application firewalls
  - Etc.
- Basically, more tools

Client-side attacks

Got protection?



What does this mean?

- The perimeter changed
- Our defenses didn't
- Antivirus to the rescue?

The New York Times hack

HOME PAGE | TODAY'S PAPER | VIDEO | MOST POPULAR | U.S. Edition

Subscribe: Digital / Home Delivery | Log In | Registe

THE AMERICANS FX

The New York Times

Wednesday, January 30, 2013 Last Update: 11:14 PM ET

Search

Follow Us | Subscribe to Home Delivery | Personalize Your W

WORLD
U.S.
POLITICS
NEW YORK
BUSINESS
DEALBOOK
TECHNOLOGY
SPORTS
SCIENCE
HEALTH
ARTS
STYLE
OPINION

Autos
Blogs
Books

Hackers in China Attacked The Times for Last 4 Months

By NICOLE PERLROTH
9:19 PM ET

The timing of the attacks coincided with reporting for an investigation that found that the relatives of China's prime minister had accumulated a fortune worth several billion dollars through business dealings.

The Opinion Pages

FIXES
The Way Out of Debt
New York City's Financial Empowerment Centers help poor clients take control of their finances, and are a model for the nation.

OP-ED CONTRIBUTOR
Treat Greed as a War Crime
Avarice and exploitation are the root of Africa's problems.

OP-ED COLUMNISTS
- Friedman: It's P.Q. and as Much as I.Q.
- Brooks, Collins: Spring Sequester
- Bittman: Lawns Into Gardens

MORE IN OPINION
- Editorial: Gun Violence
- Taking Note: The Dange Game
- Op-Ed: Palestine Shoul Take Israel to Court

Symantec Statement Regarding New York Times Cyber Attack

Created: 31 Jan 2013 | 8 comments

Symantec Corp.

0
0 Votes

Symantec. | Official Blog

Share Share Tweet Like 19

As a follow-up to a story run by the New York Times on Wednesday, Jan. 30, 2013 announcing they had been the target of a cyber attack, Symantec (NASDAQ: SYMC) developed the following statement:

"Advanced attacks like the ones the New York Times describe in the following article, (http://nyti.ms/TZtr5z), underscore how important it is for companies, countries and consumers to make sure they are using the full capability of security solutions. The advanced capabilities in our endpoint offerings, including our unique reputation-based technology and behavior-based blocking specifically target sophisticated attacks. Turning on only the signature-based anti-virus components of endpoint solutions alone are not enough in a world that is changing daily from attacks and threats. We encourage customers to be very aggressive in deploying solutions that offer a combined approach to security. Anti-virus software alone is not enough.

So how did we get here?

- Human nature
  - Easier to buy tools than to work hard
  - Bad prioritization
- Defense isn't sexy

"Put another way, n people want to fix security holes, 10n people want to exploit security holes, and 100000n want Tetris."

(Dan Kaminsky)

But we patch, right?

Well, sort of but...

- We do it slowly
- Sometimes we can't patch
  - Legacy systems
  - 3rd party systems

HD Moore's law

What about 0-days?

The Microsoft report

Microsoft

Software Vulnerability Exploitation Trends

Exploring the impact of software mitigations on patterns of vulnerability exploitation

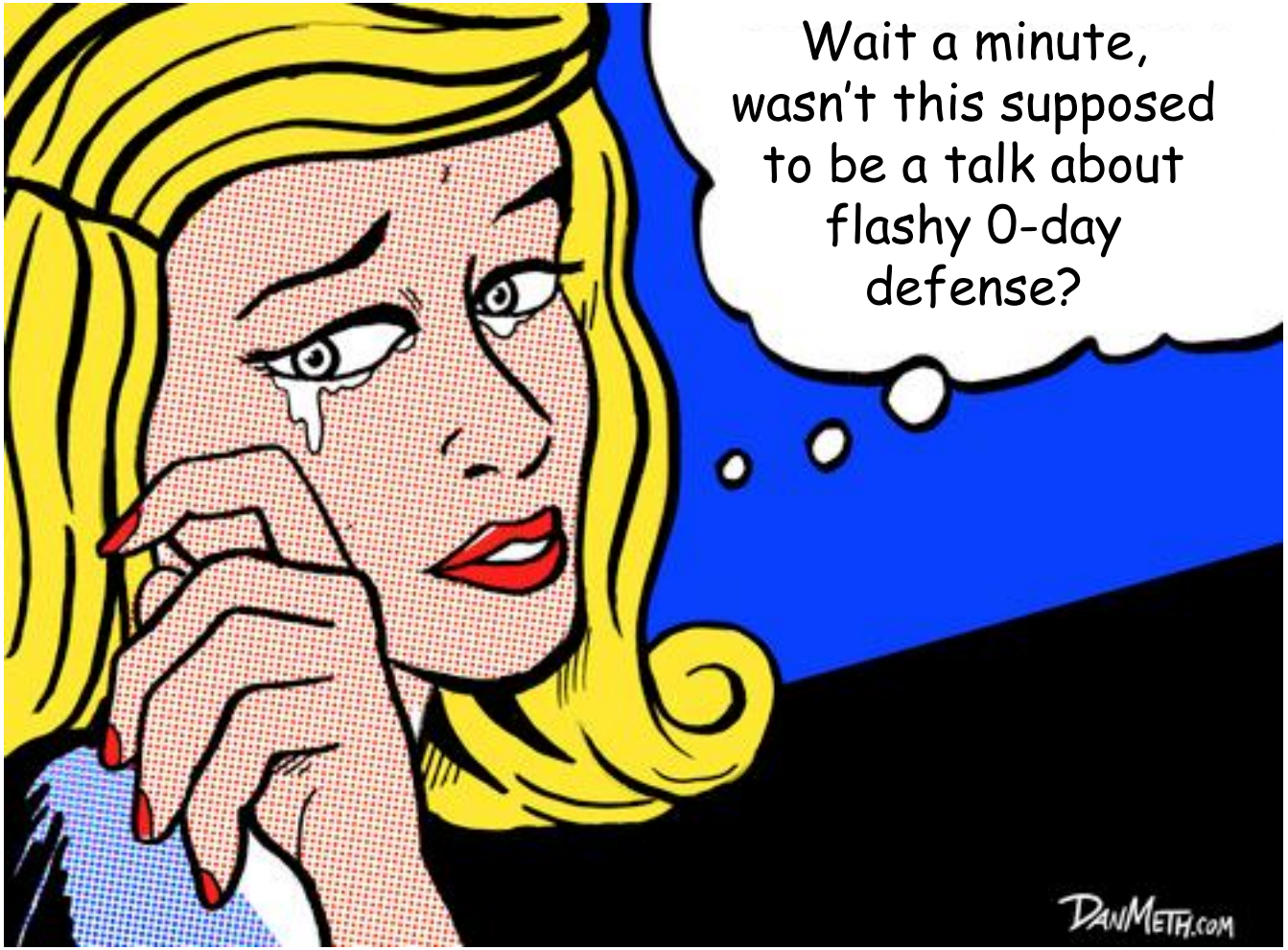
This can't be good...

- 46% of Remote Code Execution vulnerabilities exploited before patch available in 2012

Source: Software Vulnerability Exploitation Trends

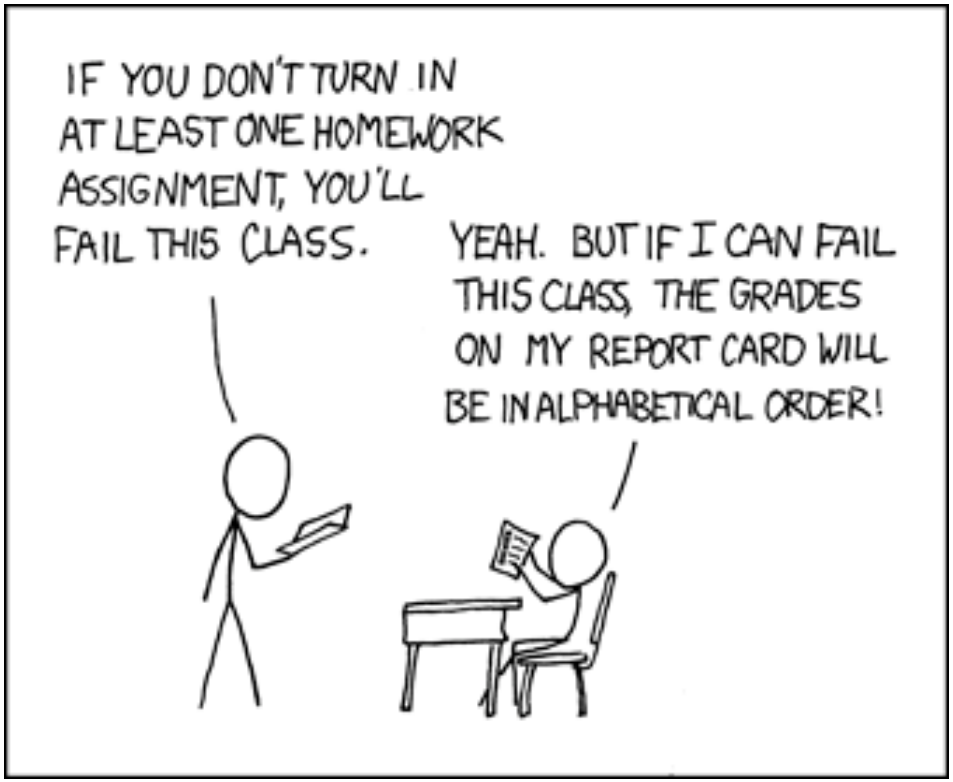
...and remember this?

- Dec 2012 – Jan 2013
- The watering hole attack


Wait a minute, wasn't this supposed to be a talk about flashy 0-day defense?
DanMeth.com

There is no flashy fix.

Priorities, priorities

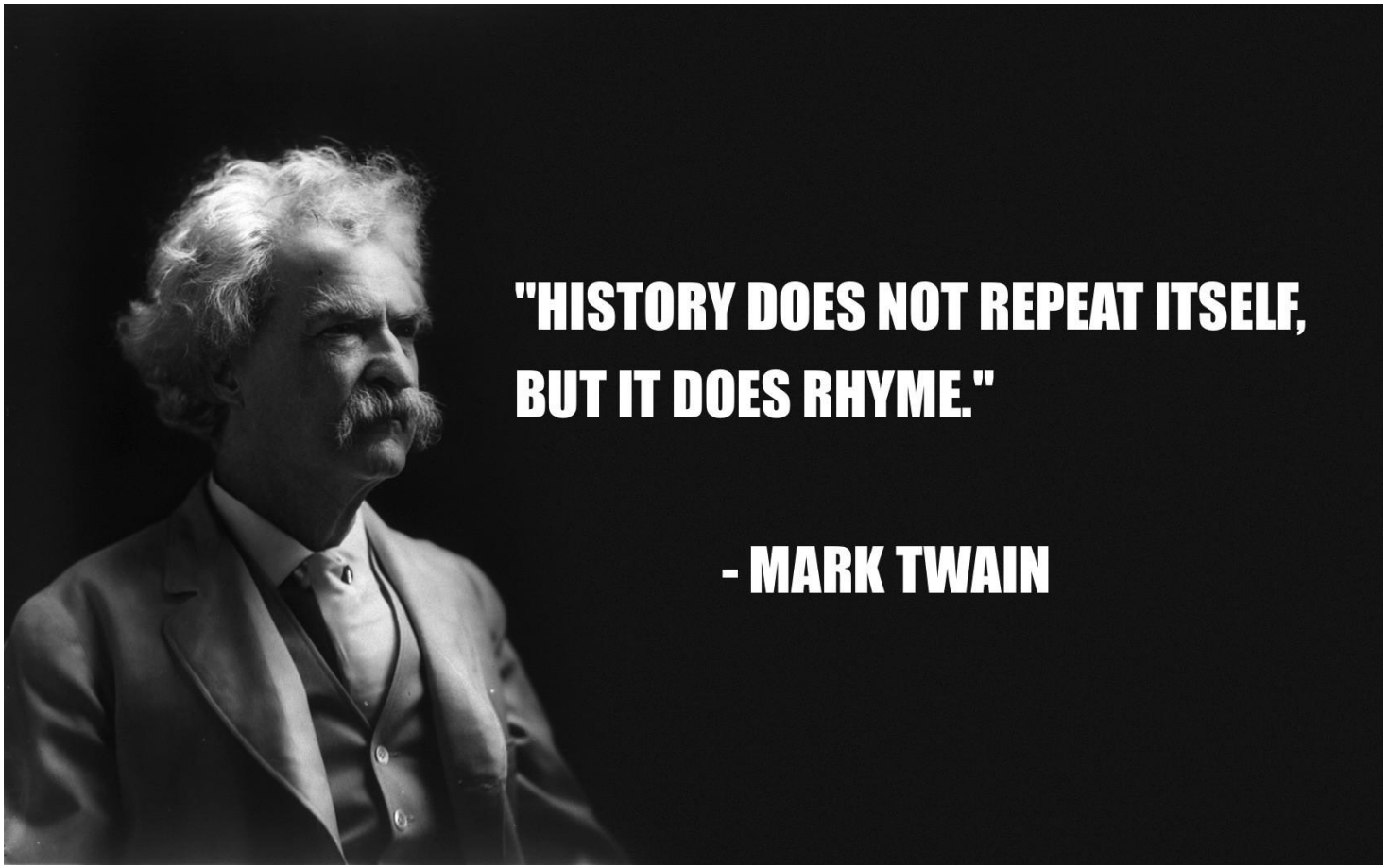


Back to basics

- Get re-acquainted with our environments
- Start using the tools we already have
- Focus on what matters

Hardening

- Usually only done high level
- Not that effective anymore
- Why don't we do it to software?


"HISTORY DOES NOT REPEAT ITSELF,
BUT IT DOES RHYME."
- MARK TWAIN

Learning from history

- Where?
- What?
- Exploitability?
- Protection?

Software hardening

- Exploit mitigation
  - ASLR, DEP, EMET, etc.
- Secure configuration
  - Software Restriction Policy
  - Native security settings

Does it work?

- The Exploit intelligence Project
- Statistics for 2009-2010:

Exploit and related defenses	No. of exploits
Memory corruption	19
Defeated by data execution prevention	14
Defeated by address space layout randomization	17
Defeated by the Enhanced Mitigation Experience Toolkit	19
Logic flaws	8
Defeated by not using Java in the Internet zone	4
Defeated by not including EXEs in PDFs	1
Defeated by not using Firefox or Foxit Reader	2

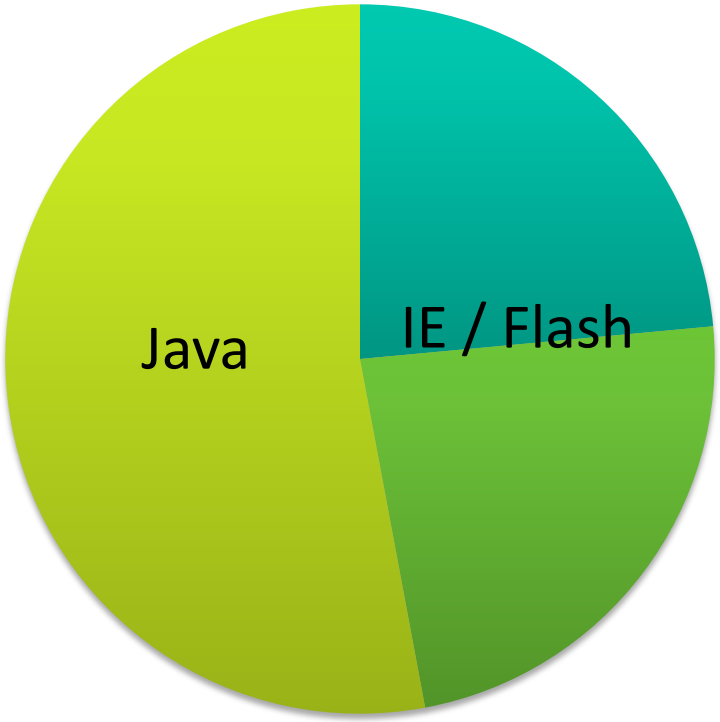
Does it work now?

- Better native defenses
  - WinXP vs Win7
  - IE7 vs IE9
- Reduced # of attack vectors being used in mass attacks

Source: The Exploit Intelligence Project

Exploit origins

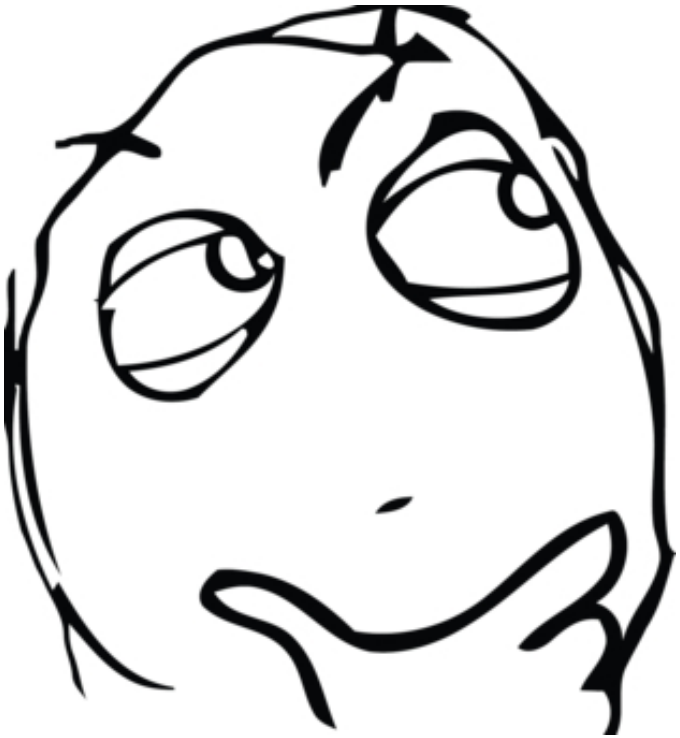
- **All** memory corruption exploits came from APT campaigns or the VUPEN blog
- **All** Java exploits came from security researchers



VUPEN Blog Articles
APT Campaigns
Security Researchers

Source: The Exploit Intelligence Project

Are we secure yet?



More hardening

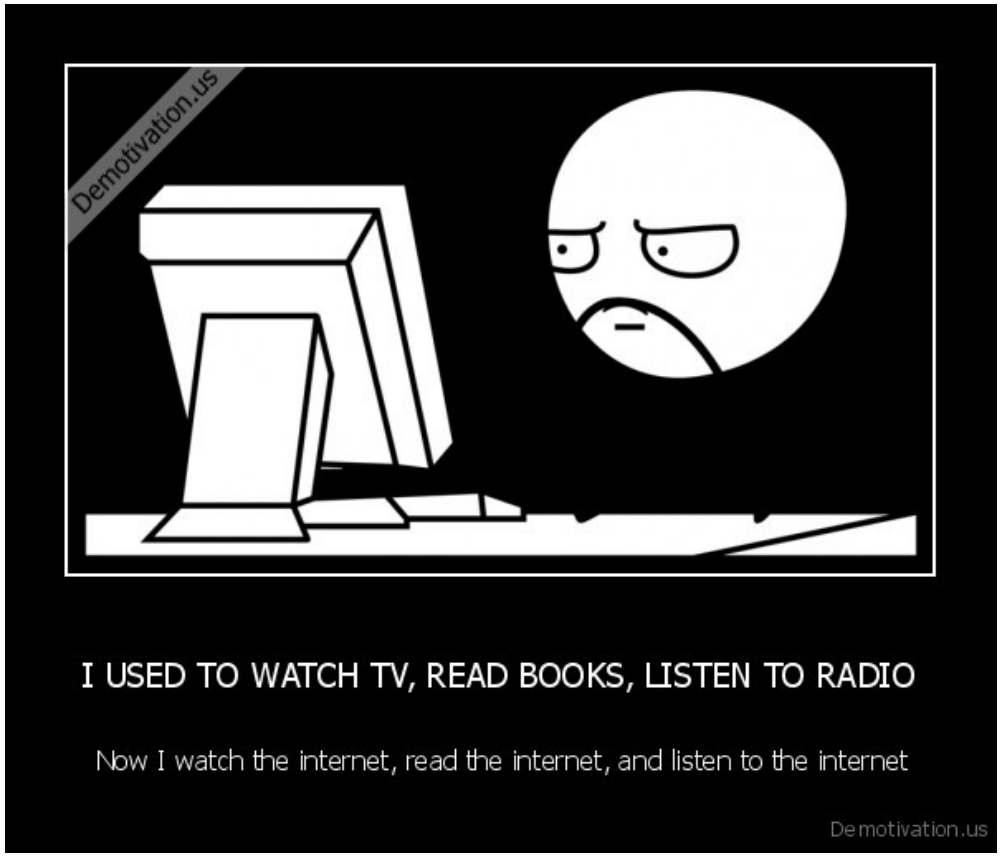
- System
- Network
- People

  and process

Reducing exposure

- Hardening will proactively reduce the risk scale of the Window Of Exposure.
- But what about when things inevitably change?

Threat intel

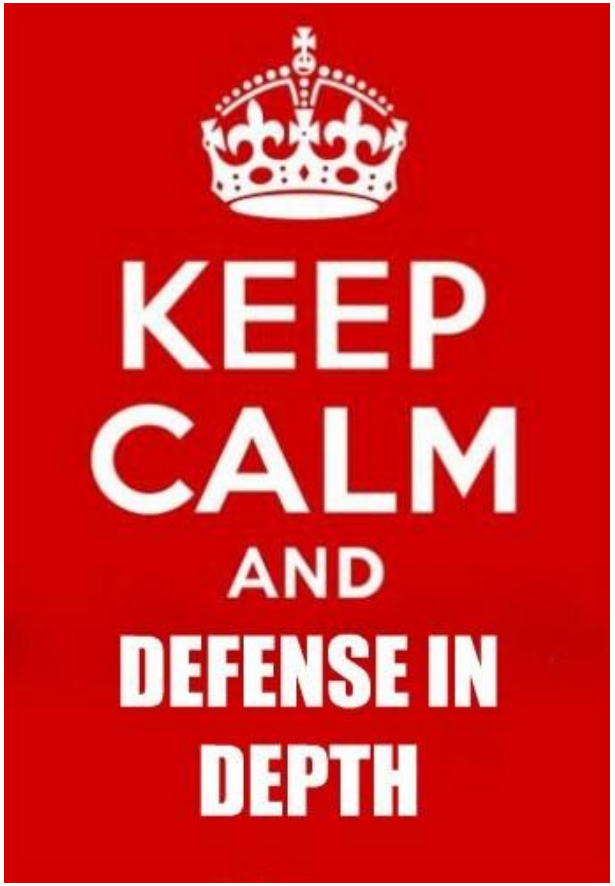


Plug the gaps

To summarize

- Priorities is key
- We need to get back to working with our environments
- This work is never done

Finally



(where it counts)

Questions?

- Contact
  - Email: andreas.lindh@isecure.se
  - Twitter: @addelindh
  - Phone: +1-555-YEAHRIGHT
- Sources:
  - Software Vulnerability Exploitation Trends: http://www.microsoft.com/en-us/download/details.aspx?id=39680
  - The Exploit Intelligence Project / Dan Guido: http://www.trailofbits.com/research/#eip