Dr. Stuxlove_

(Or How I Learned to Stop Worrying and Love the Worm)

Davi Otteheimer

flyingpenguin

Introduction

Why worry? (The RED Threat)

Yeeeeeah Haaaah!

AGENDA_

flyingpenguin_

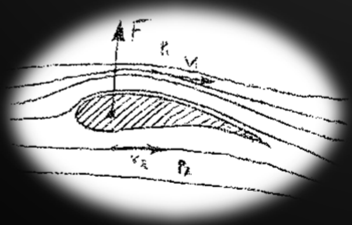
# Davi Ottenheimer

> MSc Intl History, LSE
  - Who, what, where, when
  - Cold War – Horn of Africa

> Seventeenth year in Cyberwar

> Veteran of Battle for Windows NT

# *flying*?



Dr. Strangelove_

1. USAF General Declares Strike
2. Bombers Engage, Lock-Down
3. President Tries to Recall
4. Code Unknown
5. Bombers Hit by SAM
6. Recall Code Sent
7. …one B-52 continues off-li

Yeeeeeah Haaaah!

Dr. Strangelove_

USAF Special Film 1236_

# Deterrence = power*

# Fail-safe controls

Major Kong

“Well I've been to one world fair a picnic and a rodeo and that's the stupidest thing I ever heard come over a set of earphones.”

* http://www.gwu.edu/~nsarchiv/nukevault/ebb304/

w0rms and 0-days

WHY WORRY?
(THE RED THREAT)_

Risk_

- # Vulnerabilities
- # Threats
- # Assets

- # R = (VTA)/C
  …so (R/C)V = T&A

Vulnerabilities_

# First time is the best…

# Patches, patches and patches

> Risk-based assessment

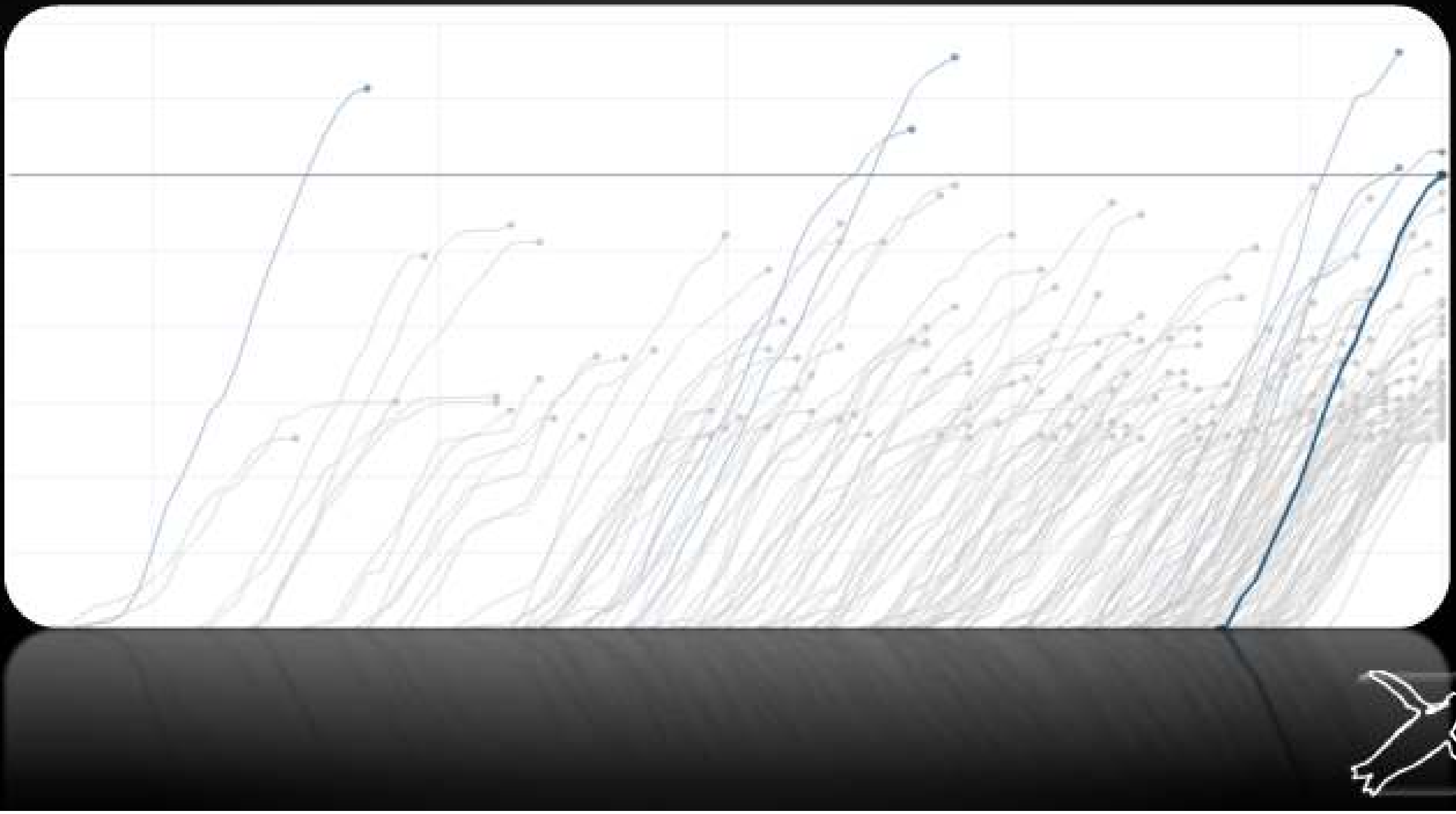
> Prioritized list

Microsoft Response Communications: “…every environment is different, we do recommend that customers evaluate accordingly…”

# Have a nice 0-day

Vulnerabilities_

# NIST CVE Trends http://nvd.nist.gov/download.cfm



Vulnerabilities_

# Microsoft AutoRun/Play

> Four of top 10 malware in 4Q/2010

> 41% infections last 3/4 of 2010

> 25% of worms in 2010

# Patch Delayed

> Windows 7 Back-port 2009

> KB971029 “Optional” Update

“…give legitimate software vendors that used the feature time…”

http://www.computerworld.com/s/article/9208858/Microsoft_cripples_USB_drive_worms_with_new_XP_Vista_update

Feb, 2011

Waldac 2.0

w0rm time_

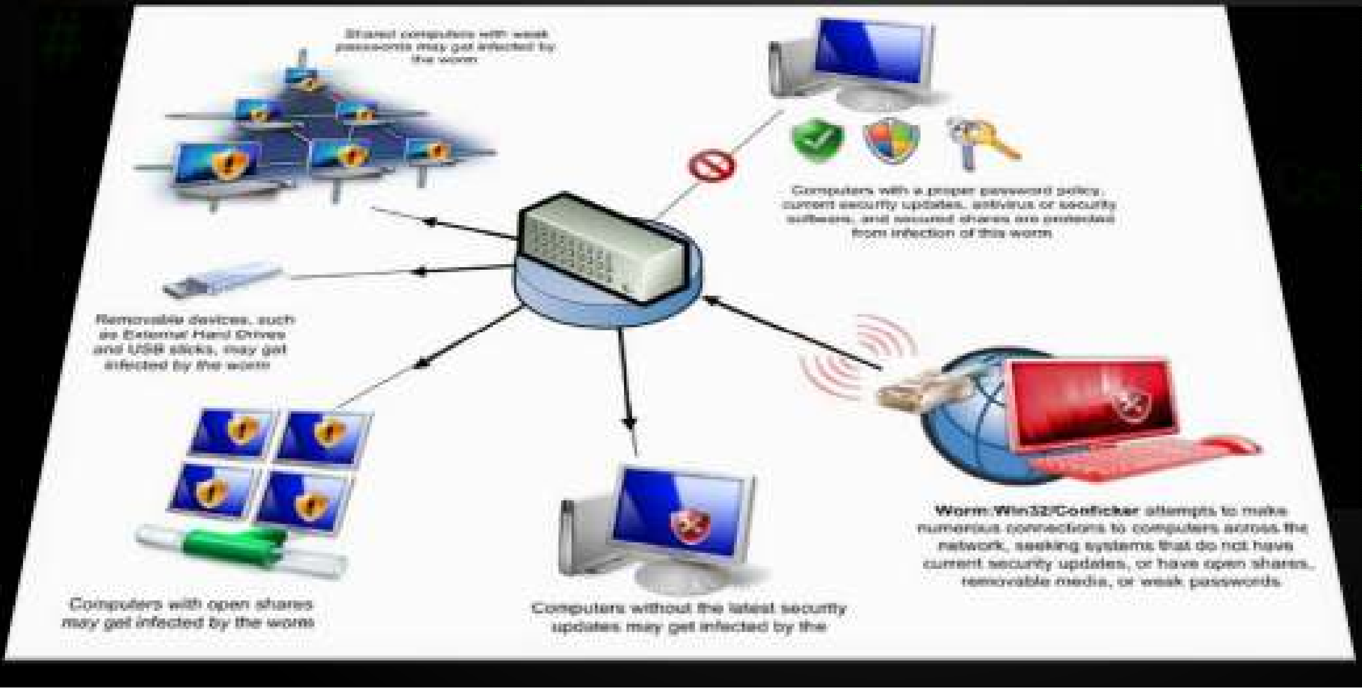
Signature?

Infections: French Navy, UK Ministry of Defence, Bundeswehr…

# Confickr (**Downup**, **Downadup** and **Kido)**

> Win32/Conficker.A November 21, 2008 (MS08-06
> Win32/Conficker.B December 29, 2008 (USB)
> Win32/Conficker.C February 20, 2009
> Win32/Conficker.D March 4, 2009
> Win32/Conficker.E April 8, 2009

April, 2009 UAE halts Siemens Step 7 controllers to Iran


Shared computers with weak passwords may get infected by the worm
Computers with a proper password policy, current security updates, antivirus or security software, and secured shares are protected from infection of this worm
Removable devices, such as External Hard Drives and USB sticks, may get infected by the worm
Worm:Win32/Conficker attempts to make numerous connections to computers across the network, seeking systems that do not have current security updates, or have open shares, removable media, or weak passwords.
Computers with open shares may get infected by the worm
Computers without the latest security updates may get infected by the

0-Day_

# Definitions

> "0 days from discovery to attack"
> "Unknown to developer"
> "No opportunity to develop a fix"

- *Byte* size change
- Segmentation offset
- 80% = Success?

"Microsoft Corp. yesterday…said it had no plans to overhaul the operating system's protocol-handling technology."[2]

4 Stuxnet 0-Day

1. MS10-046 Shell – Shortcut Ic
   - > MS07-61 Shell – URI Handling
   - > MS06-45 Shell – Folder GUID
2. MS10-061 Shell – Print[1]
3. MS10-073 – Kernel Mode
   - > Three EoP (One for XP)
   - > MS08-025 Kernel Mode EoP

FREE ISSUE TO DOWNLOAD
Hakin9
PRACTICAL PROTECTION HARD CORE IT SECURITY MAGAZINE
MY ERP GOT HACKED!
STEP-BY-STEP COMPUTER FORENSICS GUIDE
PLUS

C. Köhler
"Print Your Shell"
September 2009

[1] http://blogs.technet.com/b/msrc/archive/2010/09/13/september-2010-security-bulletin-release.aspx

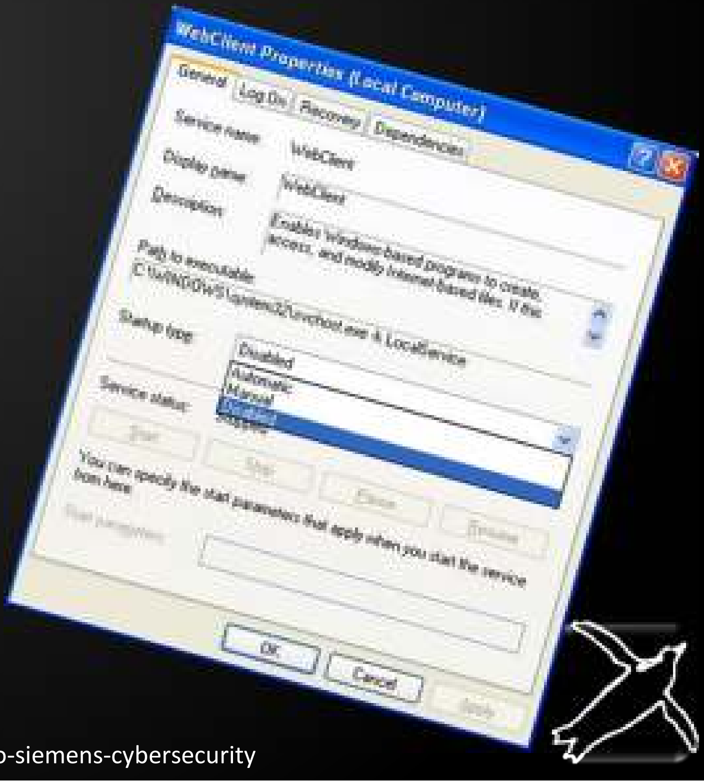
[2] http://www.computerworld.com/s/article/9042398/Microsoft_explains_Windows_URI_patch_strategy

Stuxnet 0-Day_

1. MS10-046 Shell – Shortcut Icon
   - > Local User Rights Only
   - > WebDAV Exploit

Unnecessary Services

"Microsoft wants default passwords changed…while **Siemens is telling its customers NOT to change the default passwords** as it could cause problems."*



WebClient Properties (Local Computer)

Service name: WebClient

Display name: WebClient

Description: Enables Windows-based programs to create, access, and modify Internet-based files. If the

Path to executable:
C:\WINDOWS\system32\svchost.exe -k LocalService

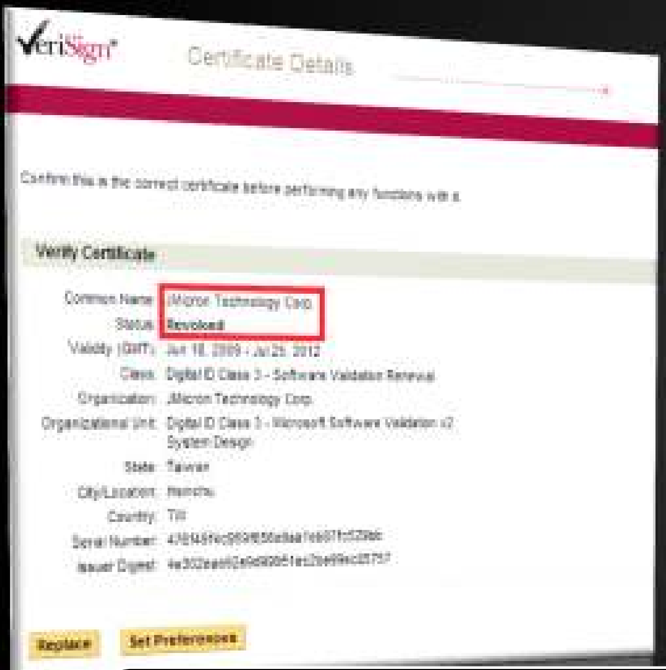
Startup type: Disabled

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

* http://community.controlglobal.com/content/just-what-are-implications-siemens-vulnerability-pauto-siemens-cybersecurity

Stuxnet Certs_



Certificate Details

Confirm this is the correct certificate before performing any functions with it.

Verify Certificate

Common Name: JMicron Technology Corp
Status: Revoked
Validity (GMT): Jun 18, 2009 - Jul 25, 2012
Class: Digital ID Class 3 - Software Validation Renewal
Organization: JMicron Technology Corp
Organizational Unit: Digital ID Class 3 - Microsoft Software Validation v2
System Design
State: Taiwan
City/Location: Hsinchu
Country: TW
Serial Number: [illegible]
Issuer Digest: [illegible]

- # Stuxnet rootkit driver signed with stolen certificate
  - > JMicron Tech Co
  - > Realtech Semi Co

"…currently tens of thousands malicious programs that have been signed – that's a fact"*

* http://www.securelist.com/en/blog/2236/Stuxnet_signed_certificates_frequently_asked_questions

Stuxnet Certs_

# 2010 Certificate Risk Study

(69 answers = “indication but not definite conclusions”)

“If malware authors would need certs they could get them”

> 69% Sign code on dev system

> 45% No password (or in batch file)

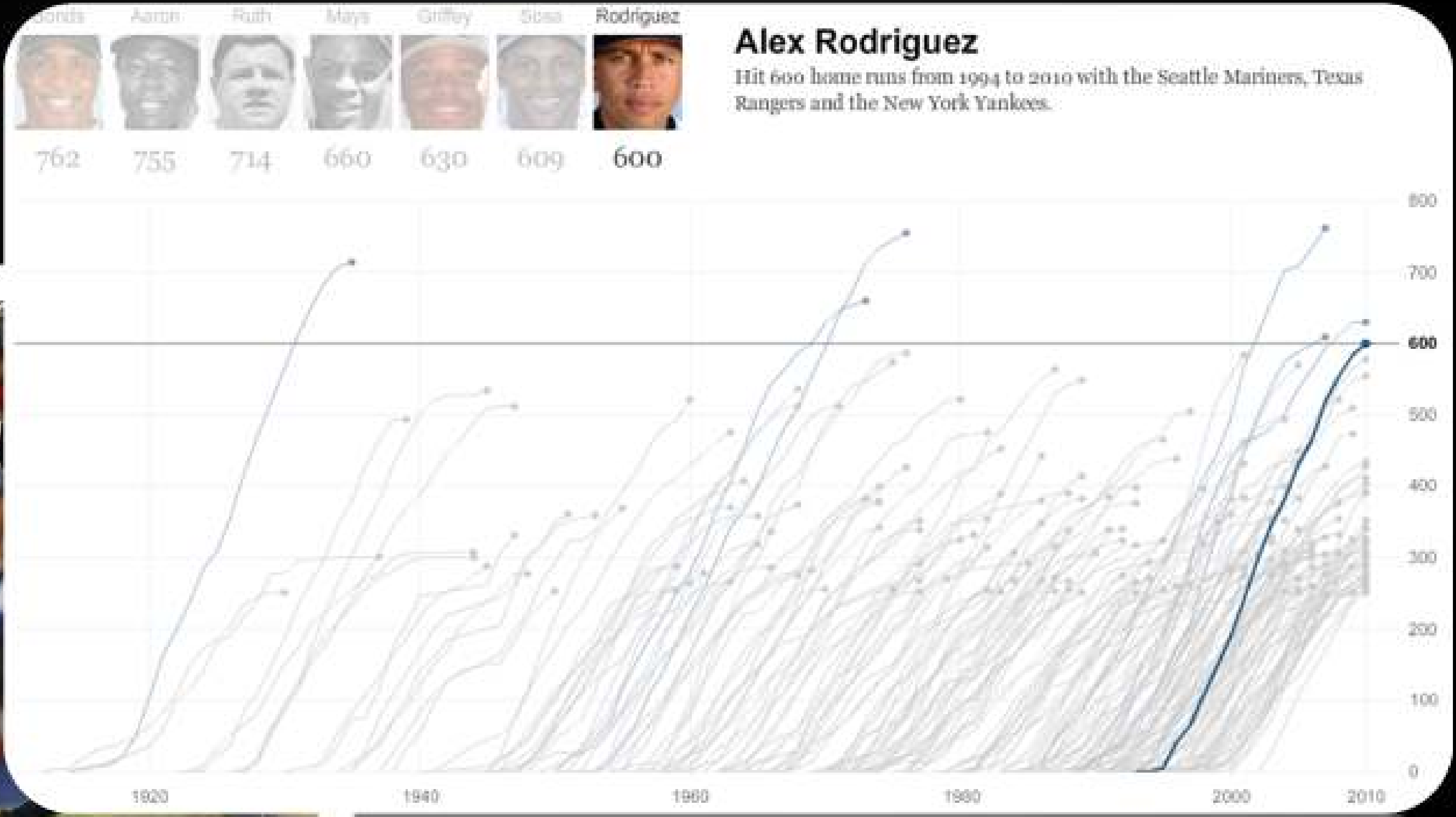
> 87% Use dev system for internet

> 12% Development system infected

http://www.f-secure.com/weblog/archives/Jarno_Niemela_its_signed.pdf

Home Run_

By Season



Bonds	Aaron	Ruth	Mays	Griffey	Sosa	Rodriguez
762	755	714	660	630	609	600

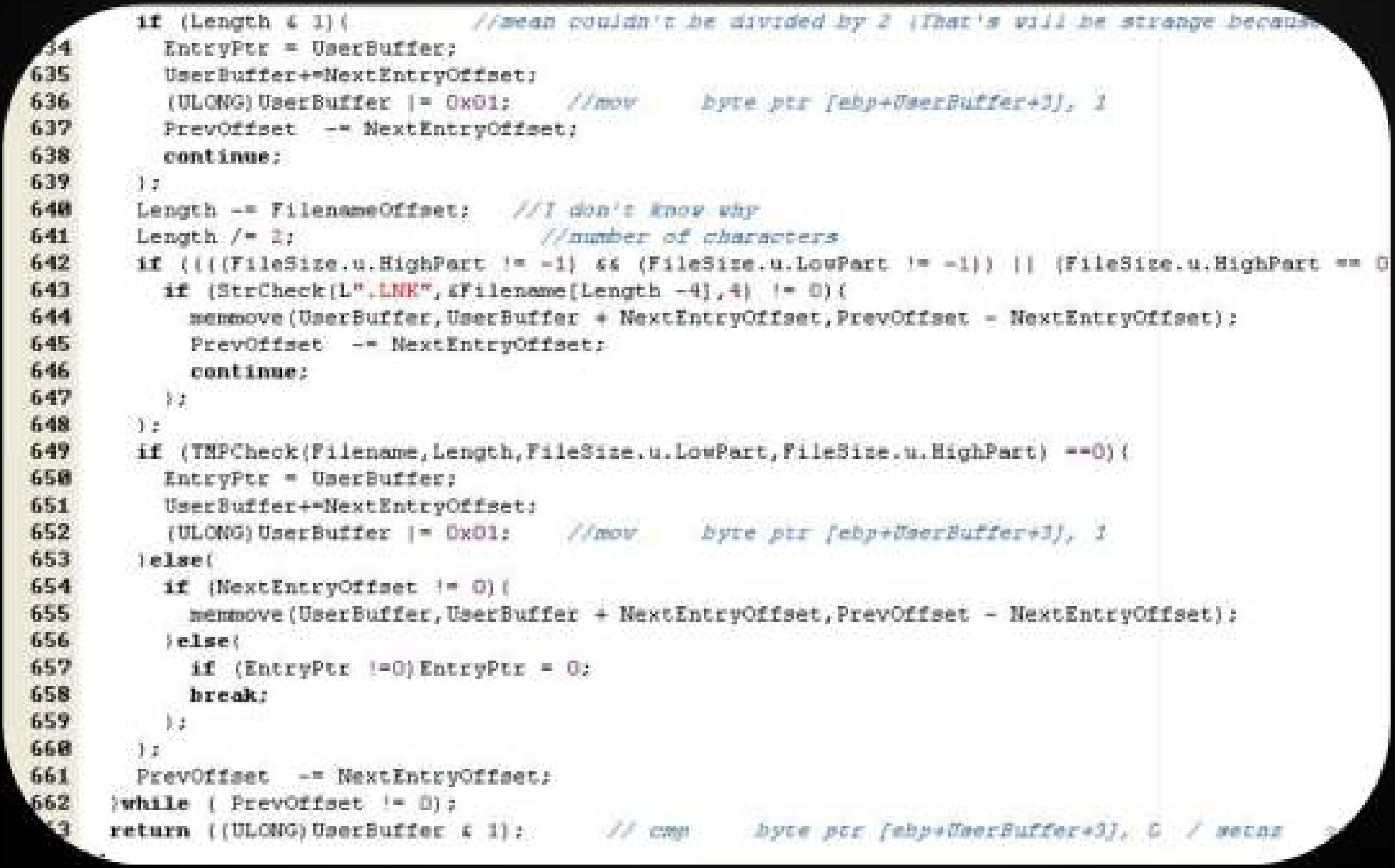
Alex Rodriguez

Hit 600 home runs from 1994 to 2010 with the Seattle Mariners, Texas Rangers and the New York Yankees.

https://www.nytimes.com/interactive/2010/07/29/sports/rodriguez-600.html

Vulnerabilities_

# Open Stuxnet Code



```
    if (Length & 1){          //mean couldn't be divided by 2 (That's will be strange becaus
      EntryPtr = UserBuffer;
      UserBuffer+=NextEntryOffset;
      (ULONG)UserBuffer |= 0x01;     //mov     byte ptr [ebp+UserBuffer+3], 1
      PrevOffset  -= NextEntryOffset;
      continue;
    };
    Length -= FilenameOffset;    //I don't know why
    Length /= 2;                    //number of characters
    if ((((FileSize.u.HighPart != -1) && (FileSize.u.LowPart != -1)) || (FileSize.u.HighPart == 0
      if (StrCheck(L".LNK",&Filename[Length -4],4) != 0){
        memmove(UserBuffer,UserBuffer + NextEntryOffset,PrevOffset - NextEntryOffset);
        PrevOffset  -= NextEntryOffset;
        continue;
      };
    };
    if (TMPCheck(Filename,Length,FileSize.u.LowPart,FileSize.u.HighPart) ==0){
      EntryPtr = UserBuffer;
      UserBuffer+=NextEntryOffset;
      (ULONG)UserBuffer |= 0x01;     //mov     byte ptr [ebp+UserBuffer+3], 1
    }else{
      if (NextEntryOffset != 0){
        memmove(UserBuffer,UserBuffer + NextEntryOffset,PrevOffset - NextEntryOffset);
      }else{
        if (EntryPtr !=0)EntryPtr = 0;
        break;
      };
    };
    PrevOffset  -= NextEntryOffset;
  }while ( PrevOffset != 0);
  return ((ULONG)UserBuffer & 1);      // cmp     byte ptr [ebp+UserBuffer+3], 0  / setnz
```

Threats_

# Cisco Global Threat Report

- > Four Security Products
- > 15K-node ScanSafe "Focus Customer"

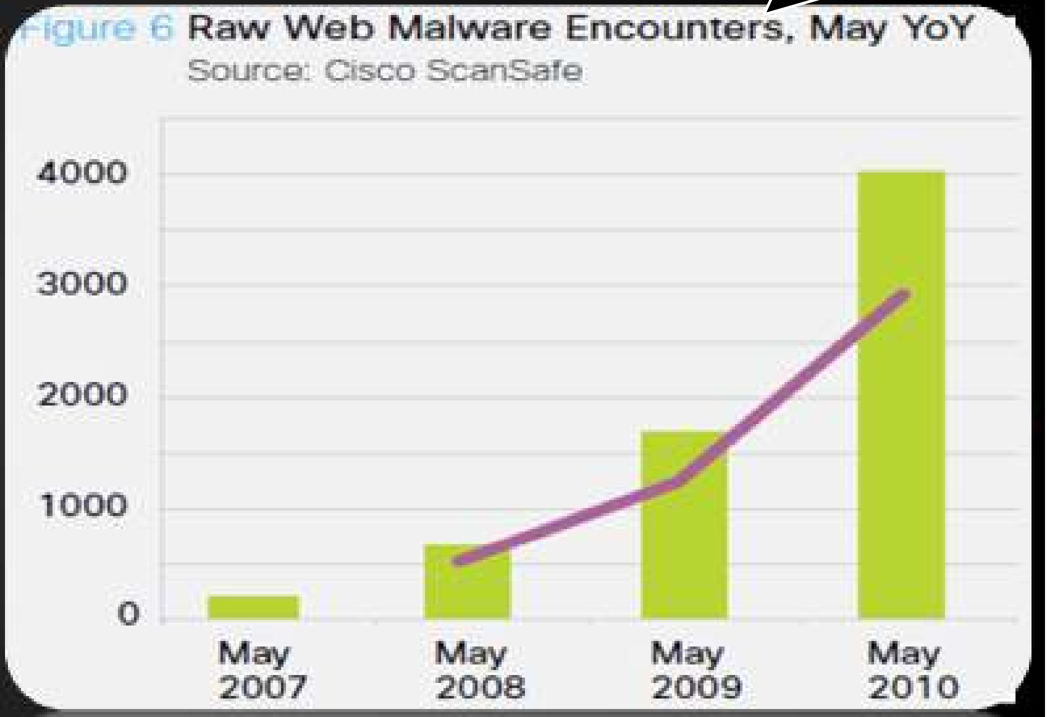


Figure 6 Raw Web Malware Encounters, May YoY

Source: Cisco ScanSafe

"…the actual rate of increase is declining."

https://www.cisco.com/en/US/prod/collateral/vpndevc/3q10_cisco_threat.pdf
https://www.cisco.com/en/US/prod/collateral/vpndevc/Cisco_Global_Threat_Report_4Q10.pdf

Threats_

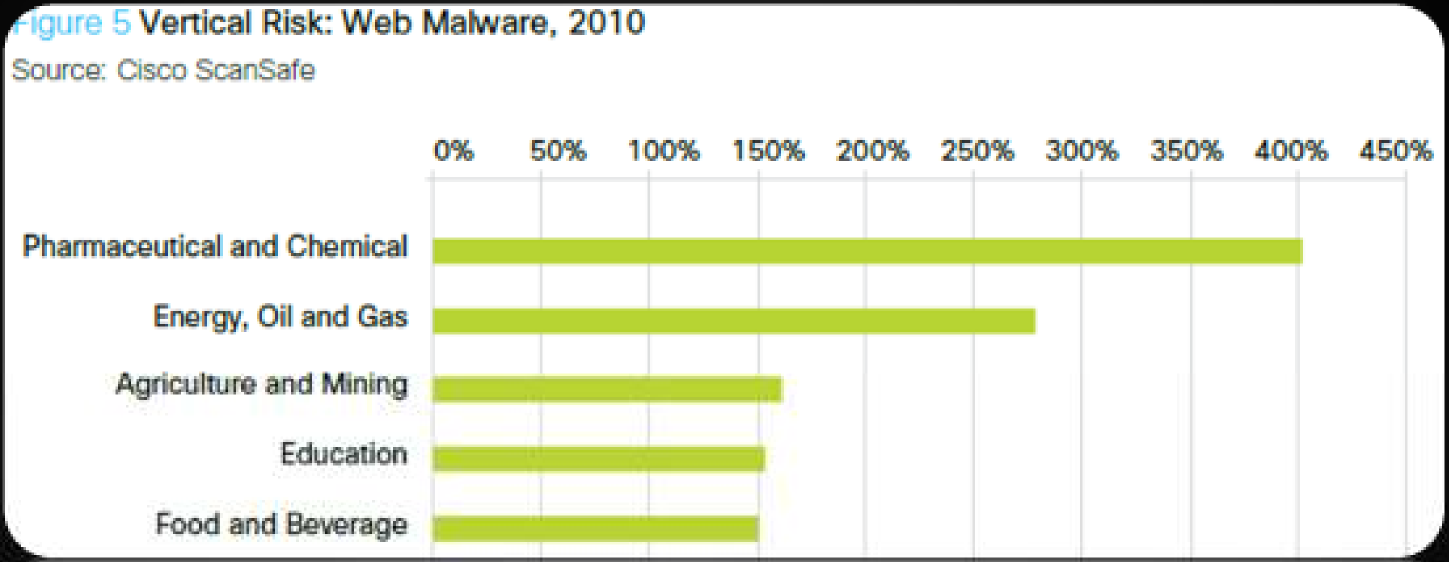


Figure 5 Vertical Risk: Web Malware, 2010

Source: Cisco ScanSafe

TrustWave

Hospitality: 38%*

Financial services: 19%

Retail: 14%

Food and beverage: 13%

Verizon

Retail: 31%

Financial services: 30%

Food and beverage: 14%

Hospitality: 6%

Other: 17%

Symantec

Education: 27%

Government: 20%

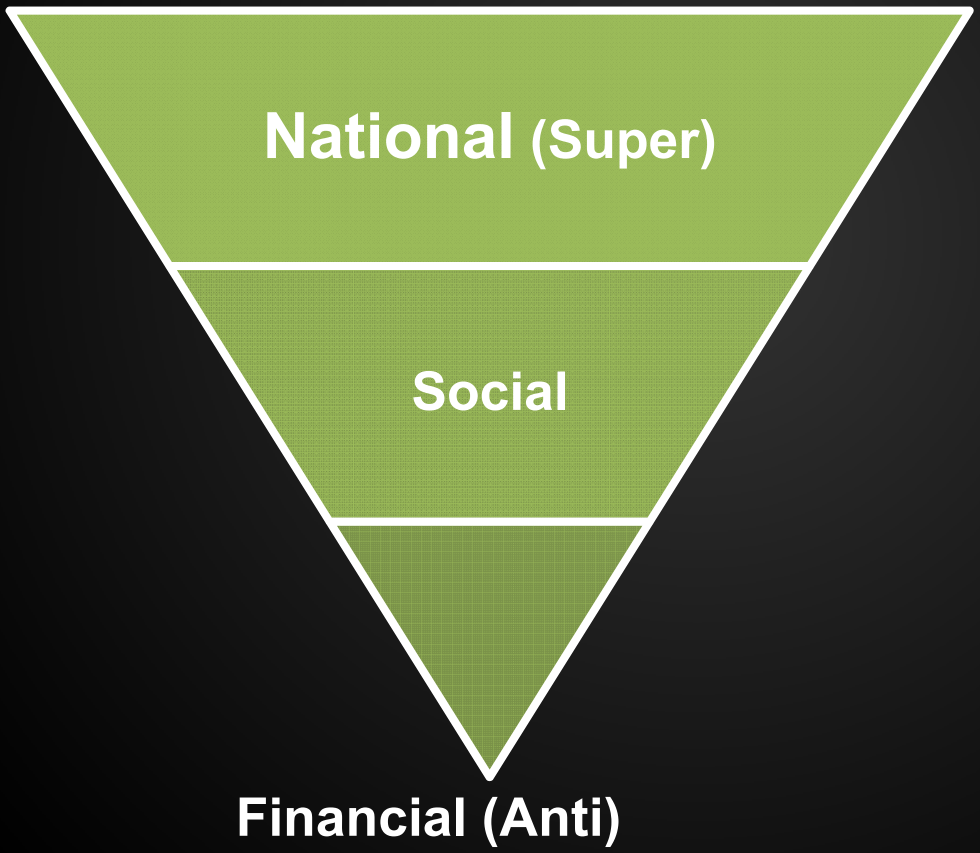
Health care: 15%

Financial: 14%

https://www.cisco.com/en/US/prod/collateral/vpndevc/Cisco_Global_Threat_Report_4Q10.pdf

Threats_

# Collaboration Levels



National (Super)

Social

Financial (Anti)

Threats_

# Insider

Rumsfeld Certainty Principle: “There are known knowns. These are things we know that we know…”

# Outsider

Gen Ripper: “Your commie has no regard for human life, not even his own. And for this reason, men, I want to impress upon you the need for extreme watchfulness.”

Threats_

# Outsider Targets (Assets)

> 2004 Titan Rain

> 2006 British MPs

> 2007 German Chancellery

> 2007 US Pentagon Email Servers

> 2007 Oak Ridge National Laboratory

> 2009 Dalai Lama

“…industries should be on high alert and take extraordinary measures to first determine if they have already been compromised, and then lock down their environments.”

Threats_

# Insider

> 2000 Vitek Boden, Maroochy Shire

> 2002 Roger Duronio, UBS Paine Webber

> 2005 Pune, India Call Centers

> 2005 Vodaphone Cell Tap, Greece

> 2008 Terry Childs, City of SF

> 2009 Stern Hu, Rio Tinto

> 2010 Bradley Manning, Wikileaks

* Dow Jones News, October 15, 1999: http://opticfiber.tripod.com/grids.html

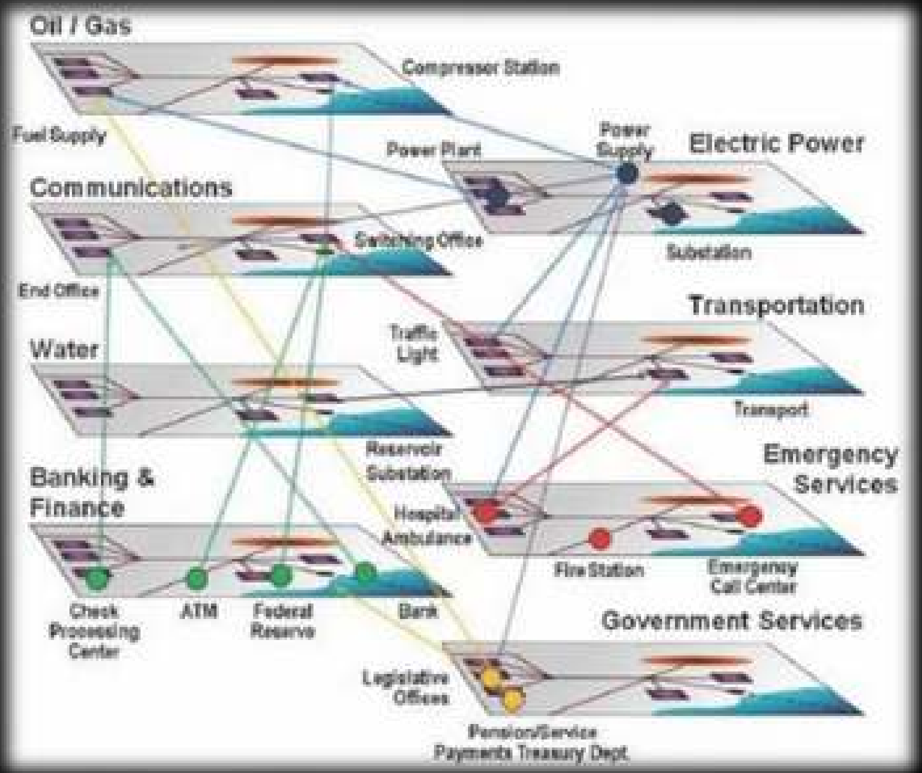
Assets_

# Critical Infrastructure

> Power

> Water

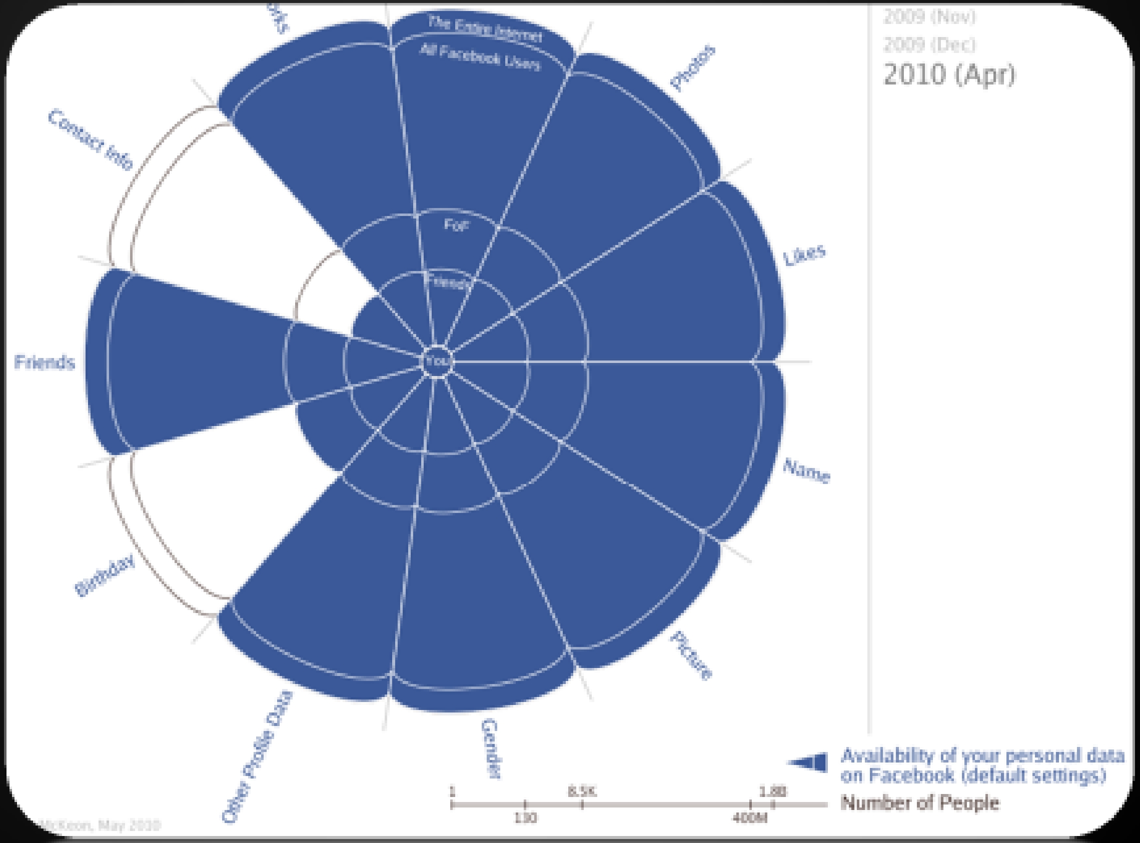
> Monuments



Sandia National LAbs

Assets_

# Privacy – Insider Information



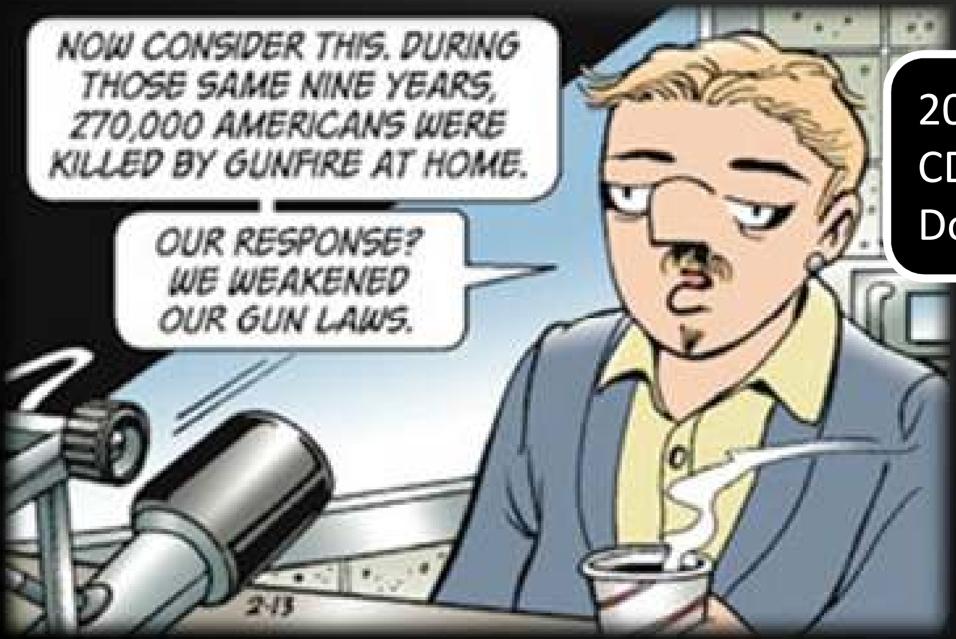
http://mattmckeon.com/facebook-privacy/

Risk Example 1_

# After 3,000 killed in 2001

> Trillions Spent, Two Wars Started

> Expansive Security Bureaucracy


NOW CONSIDER THIS. DURING THOSE SAME NINE YEARS, 270,000 AMERICANS WERE KILLED BY GUNFIRE AT HOME.
OUR RESPONSE? WE WEAKENED OUR GUN LAWS.
2-13

2003
CDC - 2,827 US Children*
DoD - 2,497 US Soldiers

* http://www.childrensdefense.org/gunrpt_revised06.pdf

Example 2_

# 73% Admit Hack 2009-2010

# 74% Admit App Security Critical

# 88% Spend More on *Coffee…*

http://www.net-security.org/secworld.php?id=10550

Pengui-matic BFC-3000

It filters
It brews
It filters some more

Stop, Drop and Roll

WHO IS WORRIED?_

Cyber-luminati?_

# Cyberwar Authors

# Auditors/PenTesters

# The Not-so-worried

1995: http://www.sjgames.com/inwo/lists/il_html2.html

Cyberwar Authors_

1. *Sophisticated* attacks

   > San Bruno Deaths = 8

   > Stuxnet Deaths = 0

"…decisions…all based on facts that were just plain wrong"
– NTSA Chair*

1982 Siberian Pipeline

2. Global warming all hype; *Cyberwar…*real!

* http://www.gjel.com/blog/new-wrongful-death-lawsuit-filed-against-pge-for-pipeline-explosion.html

Auditors / PenTesters_

# 1997 …me ☺

# 1999 Mudge “*30 Grids*”

# 2007 Idaho National Lab

# 2008 Tennessee Valley Authority

“Aurora”

Auditors / PenTesters_

# 1999 Mudge “*30 Grids*”*

“…several electric companies that stood up and said 'that's impossible...blah, blah, blah‘”

"Heck, the damn Y2K 'consultants' are much more dangerous than any mythical 'hacker‘”

* Dow Jones News, October 15, 1999: http://opticfiber.tripod.com/grids.html

Auditors / PenTesters_

"...almost all...lacked key security patches..."

# 2008 Tennessee Valley Authority

"…firewalls were either bypassed or inadequately configured, passwords were either weak or not used at all, logging of certain activity was limited, configuration management policies for control systems software were not consistently implemented, and servers and workstations lacked key patches and effective virus protection."*

* www.gao.gov/new.items/d08526.pdf

Military Leadership_

# Chair, Joint Chiefs of Staff

“…cyber threat from China is significant and that the Defense Department needs to focus more on cyber warfare.”

“…U.S. has to ‘come to a place where…those threats are diminished, if not eliminated.’”*

* http://www.military.com/news/article/senators-say-military-cyber-ops-not-disclosed.html
http://www.theage.com.au/news/in-depth/terrors-new-frontier-cyberspace/2008/04/18/1208025468962.html

(Not-yet) Worried_

# CFO: Investment Community

# CIO: Ops Management?

# Bush Administration

> Un-Regulators

Recommended Steps to Improve CyberSecurity*

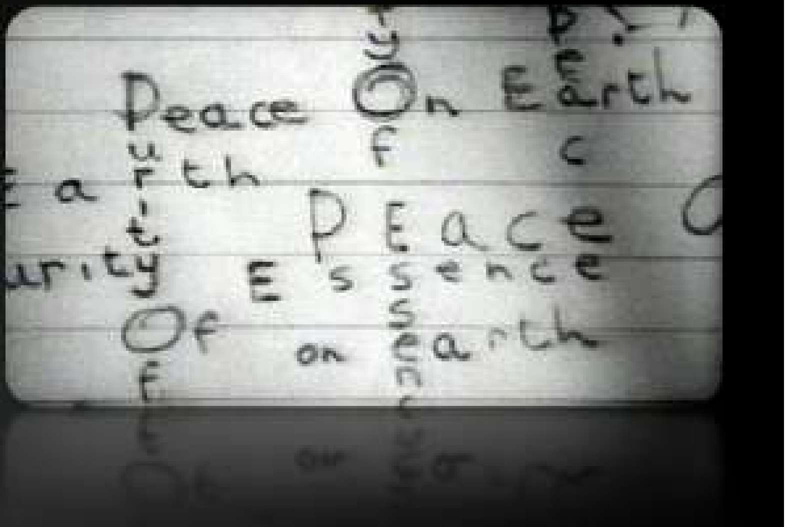
1. Identify SCADA connected to network
2. Disconnect SCADA from network

> Regulators

- NERC CIP 002-009
- NIST SP 800-82

October 2001 Executive Order 13231: President's Critical Infrastructure Protection Board

* http://www.oe.netl.doe.gov/docs/prepare/21stepsbooklet.pdf



Love the Worm?

YEEEEEAH HAAAAH!_

Reality Bytes_

# Operations Dragon and Ajax

# Global Risk

# Suggestions

# Conclusions

(Sloppy) Night Dragon_

# “Company Men”

> Beijing IPs

> Weekday 9-5 Beijing Time

> Chinese-made Tools

# Operation Sloppy Joe

> Time does not prove location

> Language does not prove identity

Operation Ajax_

# 1953 CIA-sponsored Coup in Iran

> Remove elected leader (Mossadegh)

> Restore Shah to power

> Secure Oil for UK

Operation Ajax_

# 1930s Anglo-Iranian Oil (BP)

> British profit control

> Protection from labor disputes

> Protection from audits

> No Iranian executives

> No Iranian right to annul terms

(1936 Egypt Abdicates - Riots)

Operation Ajax_

# 1948 Venezualan 50/50 Formula

> Juan Pablo Pérez Alfonso

# 1950 Saudi 50/50 Deal

> King Abdul Aziz Ibn Saud threat

> Aramco splits profit

> President Truman’s “Golden Gimmick” – 50% tax break

Operation Ajax_

# 1951 Iran Nationalizes Oil

> Truman pro-nat. (anti-communism)

> Truman pro-UK (Korean War support)

> PM Assassinated

> Mossadegh elected to PM

> UK Boycott/Blocade

# 1952 Eisenhower Elected

Operation Ajax_

# Eisenhower anti-(nationalism)

> Dulles Sec of State

> Dulles Director of CIA

“Left to themselves, these countries will reach the point where they will welcome Communism”*

# 1953 Operation Ajax

> Dismiss and Arrest Mossadegh

> Fund protests and mobs

> Pro-UK/US Shah – Dictator to ‘79

* http://www.time.com/time/subscriber/personoftheyear/archive/stories/1951.html

Global Conflict_

- # Steady Decline
- # "Extrastate" = Anti-Colonial (ended 1970s)

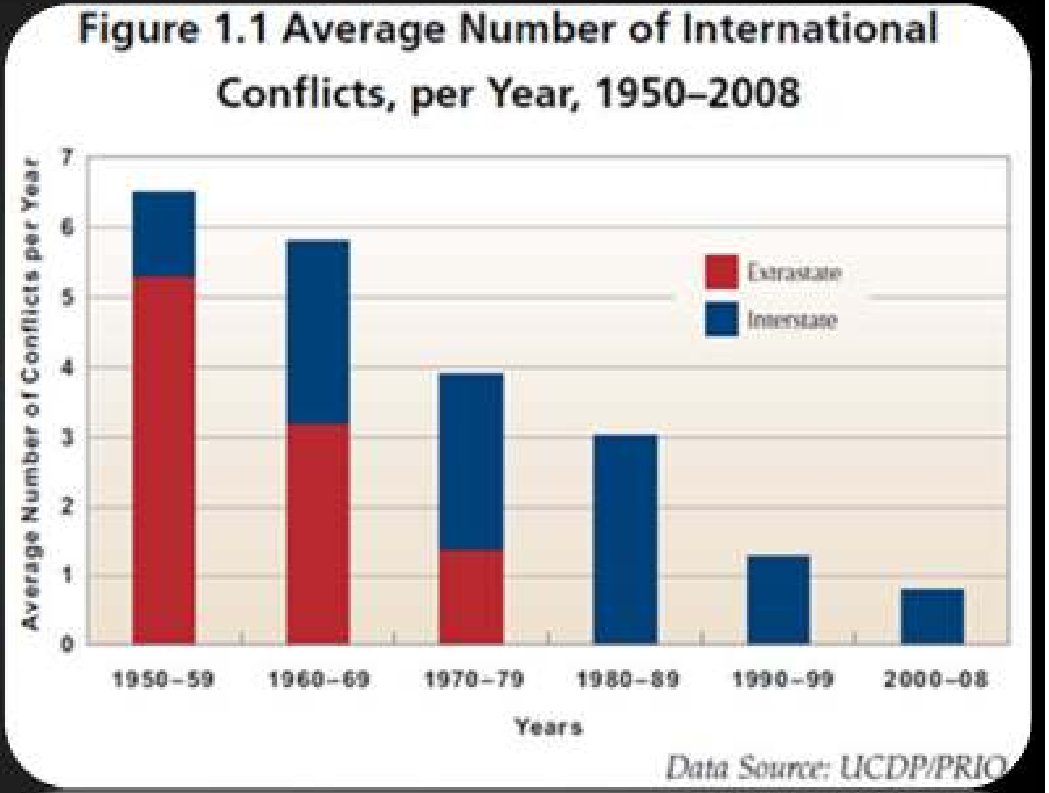


Figure 1.1 Average Number of International Conflicts, per Year, 1950–2008

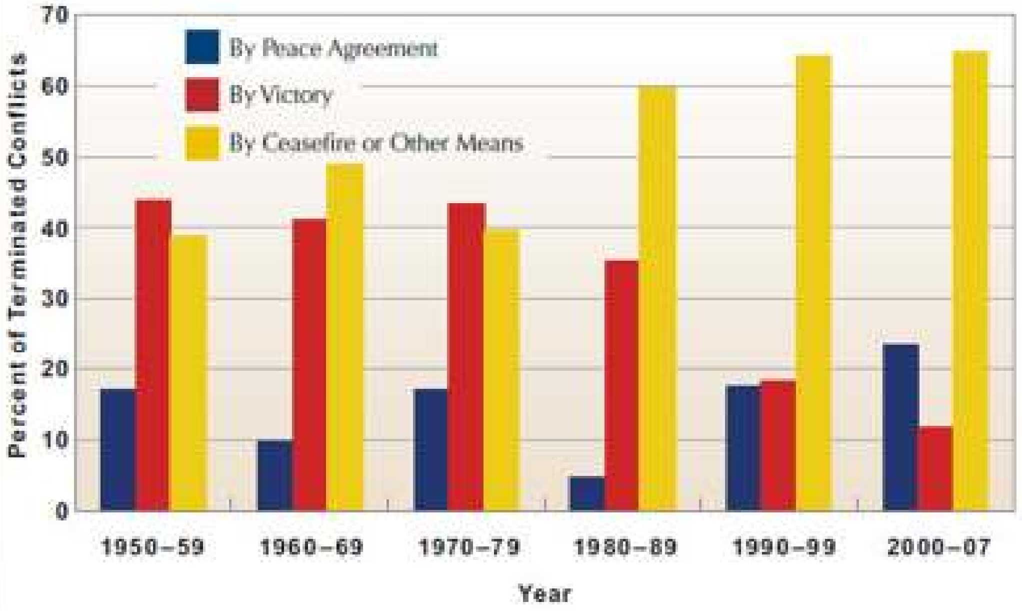
Data Source: UCDP/PRIO

http://www.hsrgroup.org/human-security-reports/20092010/overview.aspx

Global Conflict_

- # Decline in Victory%
- # Increase in Ceasefire%

Figure 4.9 Conflicts Terminated by Victory versus Conflicts Terminated by Peace Agreement, 1950–2007

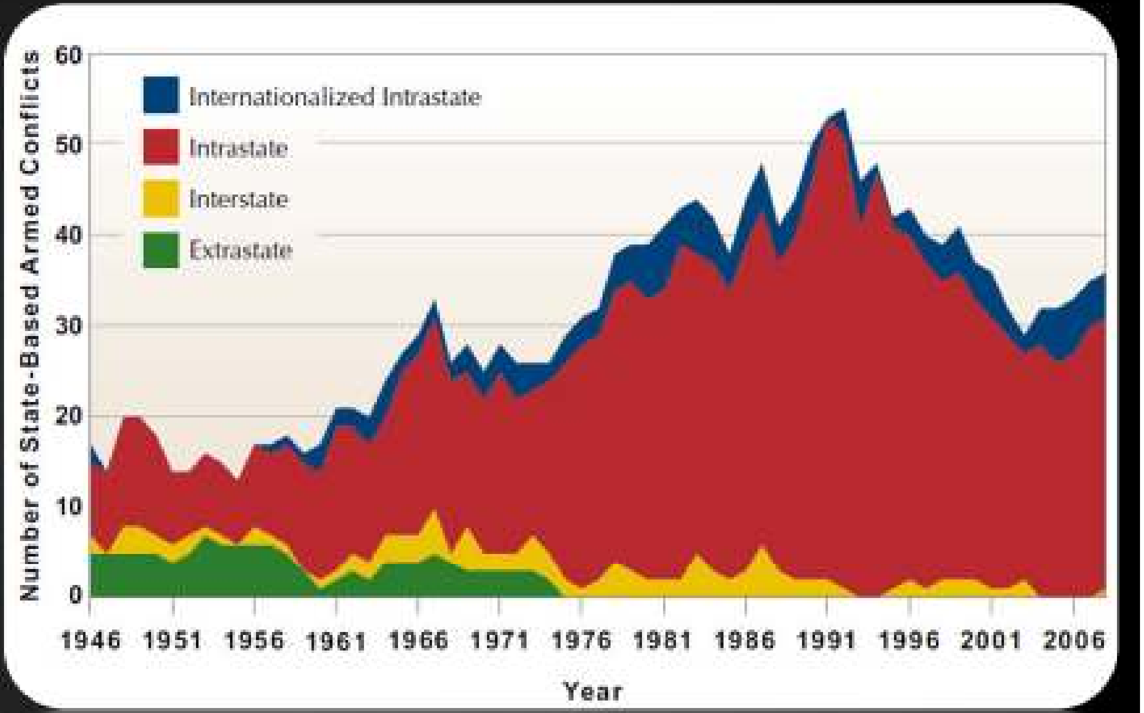


Data Source: UCDP/HSRP Dataset

http://www.hsrgroup.org/human-security-reports/20092010/overview.aspx

Global Conflict_

- # Extrastate
  - > Anti-Colonial
  - > 70s end
- # Interstate
  - > Rare post 90s



http://www.hsrgroup.org/human-security-reports/20092010/overview.aspx

Global Conflict_

- # Attribution?
- # 1989 20% of Violent Death by Non-State Actors
- # 2008 increase of 80%

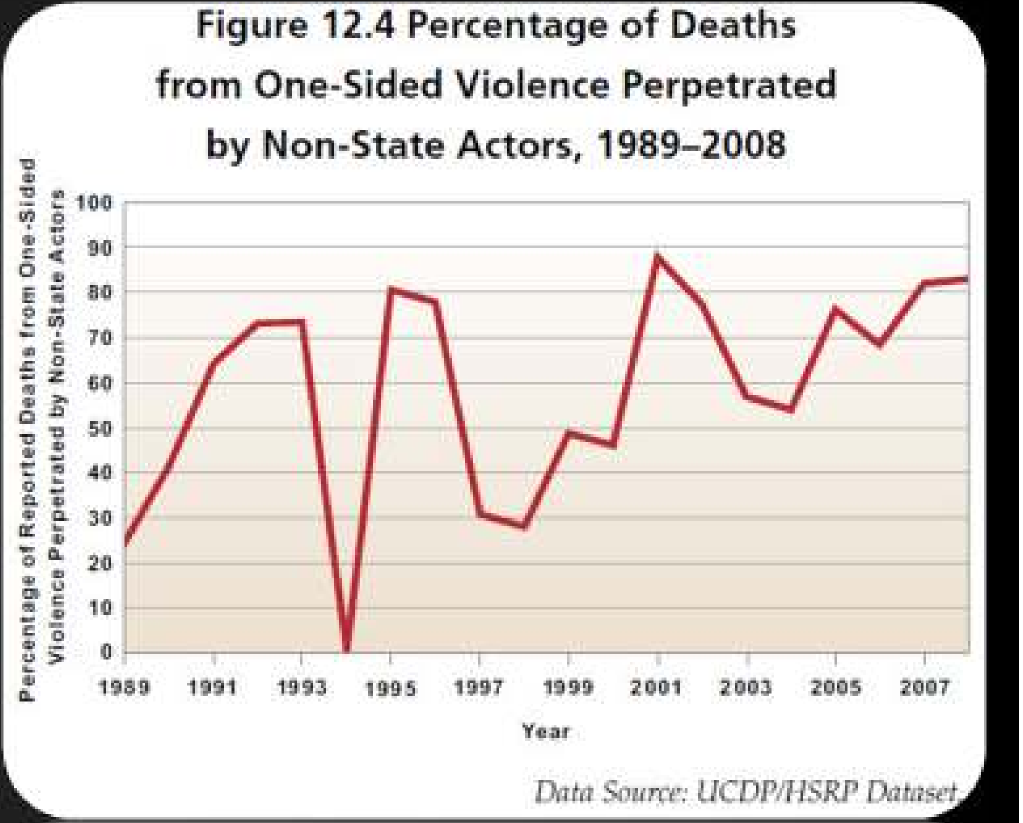


Figure 12.4 Percentage of Deaths from One-Sided Violence Perpetrated by Non-State Actors, 1989–2008

Data Source: UCDP/HSRP Dataset

http://www.hsrgroup.org/human-security-reports/20092010/overview.aspx

Assassinations_

# 2007

> Ali Reza Asgari (Unknown

# 2009

> Marivan Imam Joma

# 2010

> Massoud Ali-Mohammadi

> Majid Shahriari

> Fereydoun Abbasi

http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2009/12/the-chain-murders-1988-1998.html

Outages_

# 2008 Iran Centrifuge Failures[1]

> Pre-Stuxnet

> Trend of Success?

# 2010 Indian Point Nuclear

# 2010 Vermont Yankee Nuclear

# 2010 Moscow 500K Without Power

# 2011 Salem Township Nuclear

# 2011 Texas *50 Power Plants* Fail

[1] http://www.isis-online.org/uploads/isis-reports/documents/IAEA_Iran_Report_Analysis_18Feb2010.pdf

Fail-Safe Controls_

1. Disable Unnecessary Services
2. Use Strong Authentication
3. Patch Known Vulnerabilities
4. Monitor/Audit Logs

Windows Flight Check_

- Alternate Data Streams (ADS)
- Audit Policy status
- System file checksums
- Local User activity, dumps
- Open file handles
- Modified, Access, Created times of files on system drive
- Hidden files on the system drives
- Temporary files and cookies
- Associated DLLs of running processes
- System, application, and security logs
- Interface configuration
- Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) activity — ports opened by processes
- Local registry hive changes
- Rootkit detection
- Services running
- System information about hardware, OS, and installed software

Conclusions_

# V: No Silver Bullet

> Defense in Depth *Still* Required

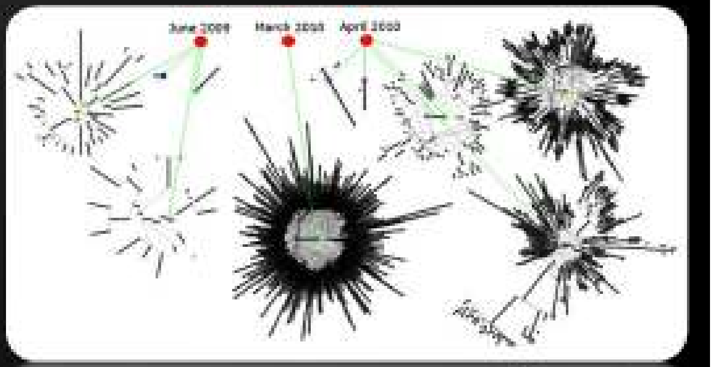
> Controls *Still* Effective

# T: Era of Super-Collaboration

> Fuzzy Attribution

> Geography Irrelevant

> No Clear Victory



http://www.symantec.com/connect/fr/blogs/updated-w32stuxnet-dossier-available

James Madison_

# The means of defence agst. foreign danger, have been always the instruments of tyranny at home.

# Among the Romans it was a standing maxim to excite a war, whenever a revolt was apprehended.

# Throughout all Europe, the armies kept up under the pretext of defending, have enslaved the people.

Constitutional Convention Speech

June 29, 1787-06-29

http://memory.loc.gov/cgi-bin/ampage?collId=llfr&fileName=001/llfr001.db&recNum=494&itemLink=D?hlaw:5:./temp/~ammem_kmli::%230010495&linkText=1

Conclusions_

# Strategic Security

> D/N Delay - Budget “Up Front” Time

> Learn (e.g. Fail) Faster

> Practice Discipline

Gen Ripper: “…war is too important to be left to politicians. They have neither the time, the training, nor the inclination for strategic thought.”

Dr. Stuxlove_

(Or How I Learned to Stop Worrying and Love the Worm)

davi@flyingpenguin.com
@daviottenheimer
415-225-7821