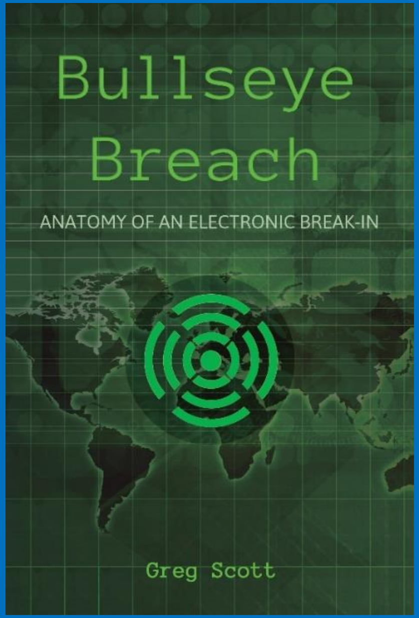
# How to prevent cybercrime in two easy steps:

## Care and share to prepare

“We’re not running a national security operation…”



# Why is anyone surprised that bad guys want to exploit today's interconnected world?

# “I don’t have time for this.  Just tell me what I need to know in 25 words or less.”

May as well just jump and learn as you go.

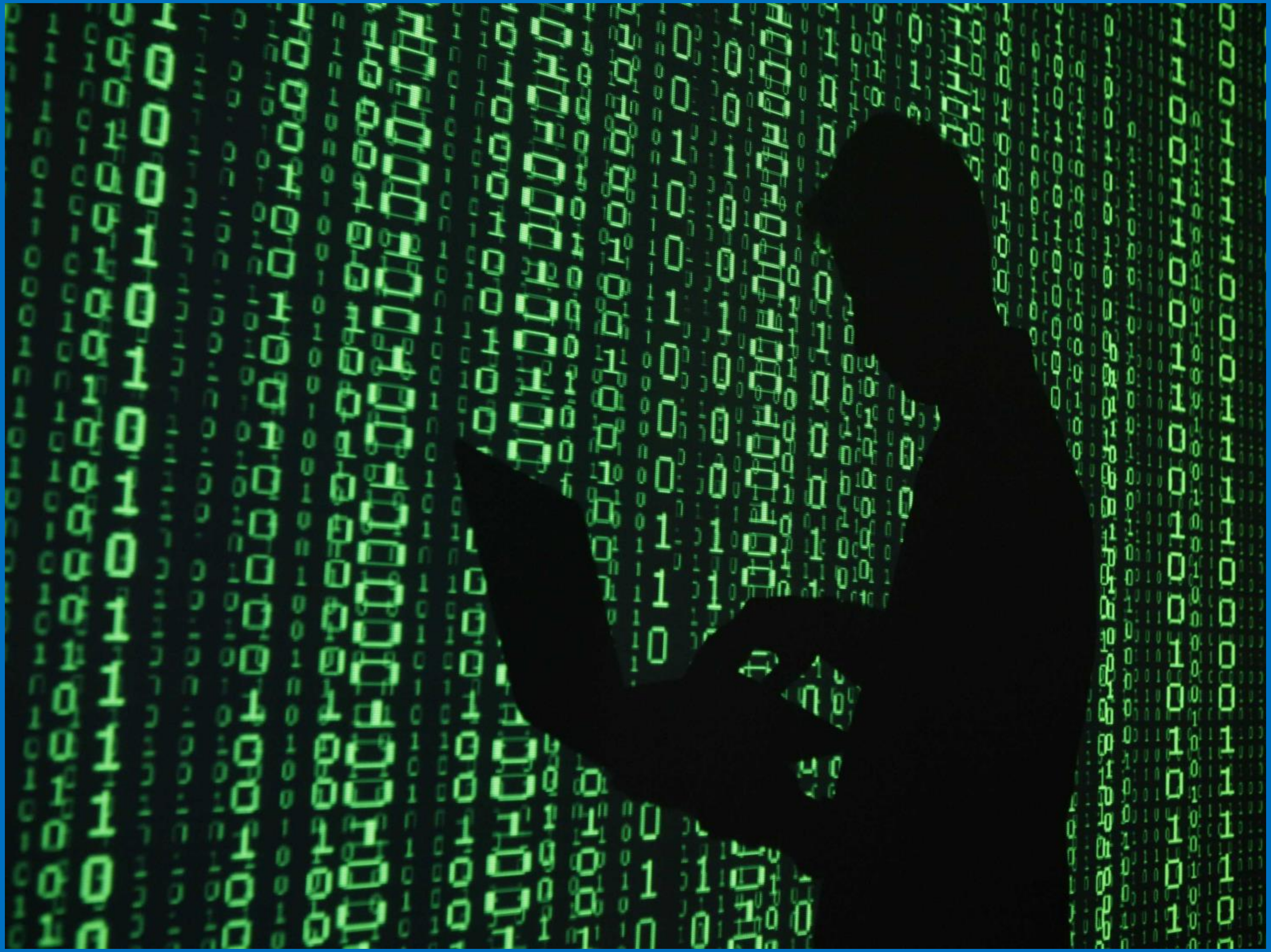
# Boring statistics that hit home

- Think of the Internet as kind of an electronic wild west.
- If you are connected to the Internet, armies of automated attackers are trying to penetrate you every minute of every day.
- In “2014 Identity Fraud Report” from Javelin Strategy & Research, more than $11 billion was reported stolen due to credit and debit card fraud in 2013, up from $8 billion in 2012. https://www.creditcall.com/wp-content/uploads/2014/07/The-Ultimate-EMV-Cheat-Sheet-Everything-ISVs-Integrators-And-VARs-Need-to-Know-About-EMV-Migration_CC1.pdf?3d8a8d

A few sobering statistics from http://www.symantec.com/security_response/publications/threatreport.jsp:

- 91% increase in targeted attacks campaigns in 2013
- 62% increase in the number of breaches in 2013
- Over 552M identities were exposed via breaches in 2013
- 23 zero-day vulnerabilities discovered
- 38% of mobile users have experienced mobile cybercrime in past 12 months
- Spam volume dropped to 66% of all email traffic
- 1 in 392 emails contain a phishing attack
- Web-based attacks are up 23%
- ***1 in 8 legitimate websites have a critical vulnerability***

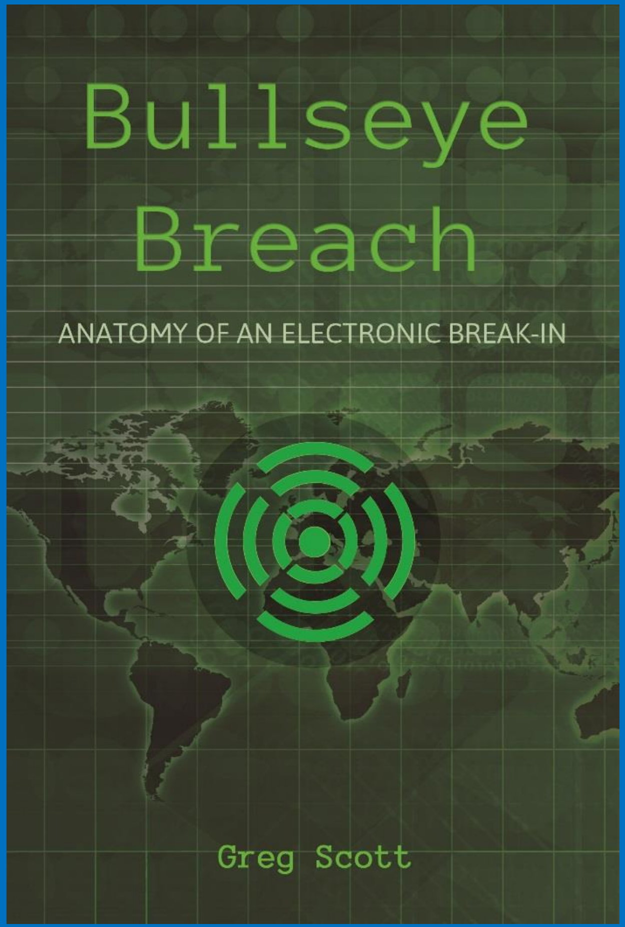
# Who are the bad guys?



# Bullseye Breach Bad Guys

- Bahir Mustafa – Iranian botnet master
- Frank Urbino – Sleazy Florida spammer
- Wai Jainde – Chinese email relay service
- Turlach Flanagan – Belfast SQL Injection specialist
- Ivan Tarski – St. Petersburg, Russia mob boss
- Fyodor Renkin – One of Ivan's protégés

And a few others you'll meet in the story



# Ivan Tarski wants to make money

- He invests in a malicious software package that compromises POS systems.
  - Point of Sale system – 21st century cash register.
- Now he needs to find POS systems to compromise.  He engages specialists to…
  - probe websites, looking for login credentials and hashed passwords
  - Probe end user computers via phishing attacks to steal passwords.
  - Match millions of username/password combinations with thousands of website/user combinations.

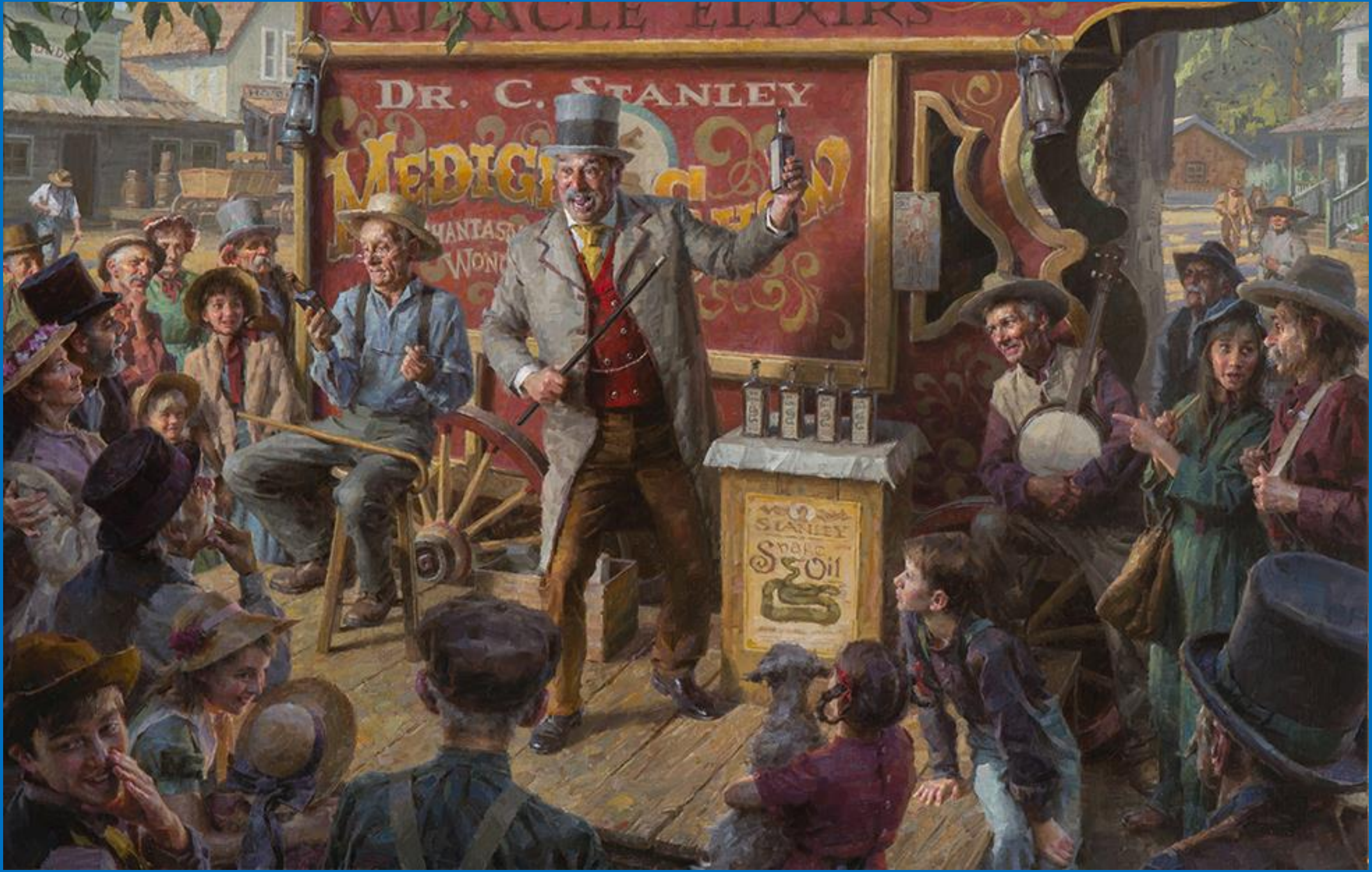
# And he finds Edith and Max Rousseau

**From:** Champlain Wireless
**Sent:** Thursday, Mar 07, 2013 4:12 AM
**To:** Edith Rousseau
**Cc:**
**Subject:** Champlain Wireless Update

CHAMPLAIN WIRELESS UPDATE

You must update your log-in info to maintain service. View attachment and continue. Thank you!

MESSAGE-ID-1HDSA-DHAS871G-DAHS671-AJ12D



Different century

Same snake oil

Image from
http://www.morganweistling.com/images/2015/WEISTLING_FINAL_REVISE_FOR_ADS_SNAKE_OIL_SALESMAN.jpg

# Max Rousseau represents everyone who thinks security is somebody else’s problem.

And that was how an obsolete, barely functional computer, sitting on a cluttered desk in a tiny family business with no secrets inside its computer network anyone cared about, became a key link in a global chain of events that shook the world.

Even if nobody wants to steal from you…

Bad guys want to use you to steal from somebody else.

And that can’t be good for business.

# Victim identified, time for deep reconnaissance.

- How are IP Addresses laid out?
- Where are the key systems?
- What are the passwords?

- After various technology attacks fail, Ivan comes up with a clever spear phishing and social engineering campaign.
- Ivan’s crew steals 40 million credit card numbers and sells them in an underground Internet marketplace.
- Of course, there’s more to the story.  (Read the book.)

# A few famous real-world attacks

- Who to pick on first?

# Send me an email on that

Don’t apprentices get fired for making excuses?

What about CEOs?

“Like virtually every other company these days, we have been alerted to potential suspicious credit card activity and are in the midst of a thorough investigation to determine whether it involves any of our properties,” the statement reads. “We are committed to safeguarding all guests’ personal information and will continue to do so vigilantly.”

http://krebsonsecurity.com/2015/07/banks-card-breach-at-trump-hotel-properties/

# When lip service turns deadly

# Office of the Inspector General, November 12, 2014, from the Final Audit Report:

https://www.opm.gov/our-inspector-general/reports/2014/federal-information-security-management-act-audit-fy-2014-4a-ci-00-14-016.pdf

System certification is a comprehensive assessment that attests that a system's security controls are meeting the security requirements of that system, and accreditation is the official management decision to authorize operation of an information system and accept its risks. OPM's process of certifying a system's security controls is referred to as Security Assessment and Authorization (Authorization.)

Not only is a large volume (11 out of 47 systems; 23 percent) of OPM’s systems operating without a valid Authorization, but **several of these systems are amongst the most critical and sensitive applications owned by the agency.**

Furthermore**, two additional systems without Authorizations are owned by OPM’s Federal Investigative Services, which is responsible for facilitating background investigations for suitability and security clearance determinations.** Any weaknesses in the information systems supporting this program office could potentially have **national security implications.**

**We recommend that the OPM Director consider shutting down information systems that do not have a current and valid Authorization.**

*U.S. Was Warned of System Open to Cyberattacks*
*http://www.nytimes.com/2015/06/06/us/chinese-hackers-may-be-behind-anthem-premera-attacks.html?_r=1*

*Hacking of Government Computers Exposed 21.5 Million People*
*http://www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html*

**If you applied for a US Government clearance between 2000 and 2015, the Chinese probably know as much about you as the United States Federal Government.**

"We take very seriously our responsibility to secure the information stored in our systems, and in coordination with our agency partners, our experienced team is constantly identifying opportunities to further protect the data with which we are entrusted," said Katherine Archuleta, director of the Office of Personnel Management.
--Wall Street Journal, June 5, 2015

Yeah, Uh-huh.

*Katherine Archuleta, Director of Personnel Agency, Resigns*
http://www.nytimes.com/2015/07/11/us/katherine-archuleta-director-of-office-of-personnel-management-resigns.html?_r=0

# Adding insult to injury

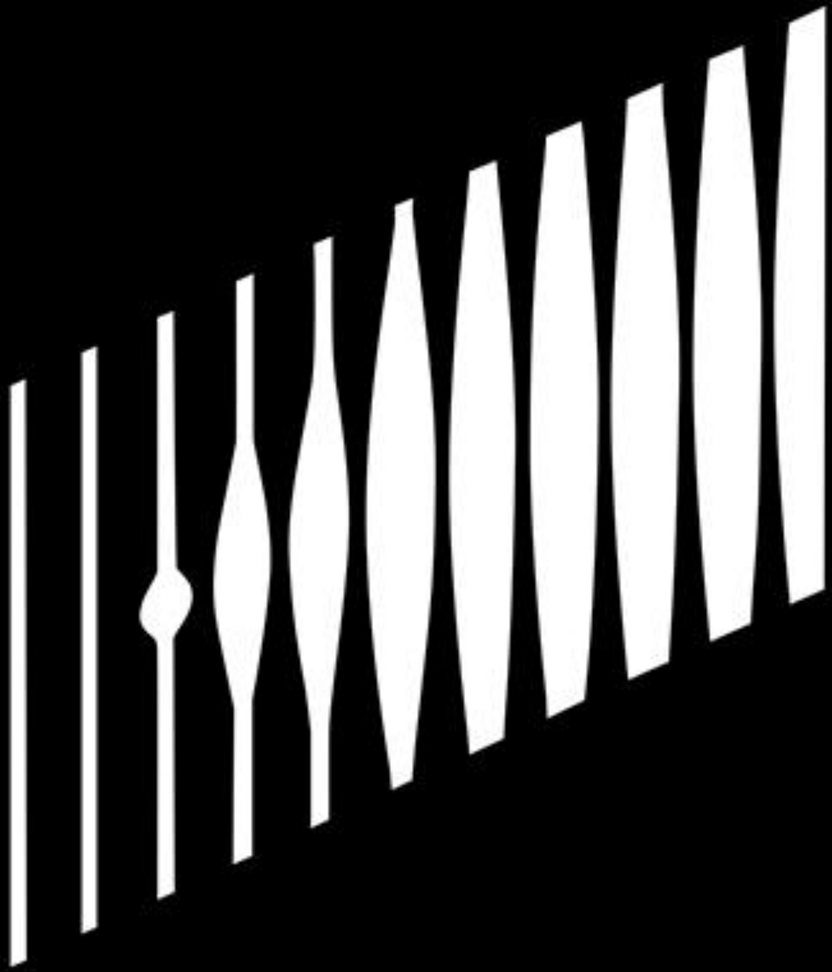
- The OPM remedy?  Send an email to Federal employees with a “click here” link to sign up for worthless credit monitoring.
- Spammers and phishers quickly jumped onto the gravy train.
  - https://federalsoup.com/articles/2015/07/02/scammers-leveraging-opms-credit-monitoring-offer.aspx
  - http://www.zdnet.com/article/phishing-e-mail-temporarily-stops-opm-hack-remediation-efforts/

# One last piece of OPM irony

- Here is the link to the National Institute of Standards' cybersecurity framework:

  http://www.nist.gov/cyberframework/

- The United States Federal Government literally wrote the book on cybersecurity. And keeps it updated.
- Apparently, nobody at the United States Federal Government Human Resources Office read it.



SONY
PICTURES

- Back in 2005 Sony was the attacker.
- Sony BMG planted root kits on consumer PCs for everyone who bought a Sony music CD.
- Mark Russinovich uncovered it.   Bruce Schneier wrote a great article.
- The class action lawsuit cost Sony $millions.
- See http://www.infrasupport.com/right-way-deal-security-vulnerability-disclosures/

T·J·maxx®

2005-2007. Attackers were inside the TJ Maxx corporate network for 18 months apparently using a laptop in a parking lot to penetrate a store wifi.

http://www.zdnet.com/article/tjxs-failure-to-secure-wi-fi-could-cost-1b/

- One of the Big 3 credit reporting agencies.
- Experian sold consumer personal information to an illegal identity theft service.
- Court Ventures sold data to a fraud friendly service named Superget.info
- Experian bought Court Ventures.
- And kept selling to Superget.info for nearly a year.
- Payments apparently came via wire transfer from Singapore.
- See [http://krebsonsecurity.com/2013/10/experian-sold-consumer-data-to-id-theft-service/](http://krebsonsecurity.com/2013/10/experian-sold-consumer-data-to-id-theft-service/)

# Internet infrastructure companies aren’t immune

- Comodo – a large CA: http://www.infoworld.com/article/2623829/authentication/weaknesses-in-ssl-certification-exposed-by-comodo-security-breach.html
- VeriSign Hacked, Successfully and Repeatedly, in 2010 https://www.schneier.com/blog/archives/2012/02/verisign_hacked.html
- More CAs Report Breaches, Suspend Issuing SSL Certificates http://www.eweek.com/c/a/Security/More-CAs-Report-Breaches-Suspend-Issuing-SSL-Certificates-479218
- This GoDaddy hack was against its web hosting operation: http://www.bleepingcomputer.com/forums/t/556918/possible-breach-on-godaddy-hosting-serves-windows-shared-hosting-accounts/

No IT security presentation would be complete without mentioning the fallout from Bradley Manning and Edward Snowden.

- NSA infiltrated RSA security more deeply than thought – study [http://www.reuters.com/article/2014/03/31/us-usa-security-nsa-rsa-idUSBREA2U0TY20140331](http://www.reuters.com/article/2014/03/31/us-usa-security-nsa-rsa-idUSBREA2U0TY20140331)
- After NSA Backdoors, Security Experts Leave RSA for a Conference they can Trust [https://www.eff.org/deeplinks/2014/01/after-nsa-backdoors-security-experts-leave-rsa-conference-they-can-trust](https://www.eff.org/deeplinks/2014/01/after-nsa-backdoors-security-experts-leave-rsa-conference-they-can-trust)
- How Worried Should we be About the Alleged RSA-NSA Scheming? [http://www.wired.com/2013/12/what-we-really-lost-with-the-rsa-nsa-revelations/](http://www.wired.com/2013/12/what-we-really-lost-with-the-rsa-nsa-revelations/)

**That’s right. The United States National Security Agency, charged with protecting our nations’ secrets, is both a perpetrator and victim.**

# Here’s where it gets personal

If you’re a cyber victim, you’re on your own.

# Twin Cities embezzlement case from the 1990s.

- I met with the IT Director at a large company to do some DEC VMS support.
- The IT Director told me that all work at this organization had to go through his favored consulting company.
- I did the work, submitted invoices, and eventually got paid.
- A few months later, Police arrested the IT Director.
    - He did a perp walk through the company cafeteria.
- Local police interviewed me about my invoices.
- Apparently, the consulting company padded my invoices and others and shared the loot with the IT Director.

- It took the FBI 5, count ‘em, 5 years to work this case.

# November 2000 attack on my DNS server.

- My very first serious foray into Linux.
- “What did you do to the Internet this time, Greg” – Tina Scott, November, 2000.
- My little DNS server was an unwitting partner in a DDOS attack against the country of Brazil.
- My friends from Mission Critical Linux helped me diagnose it and advised me to call the FBI.
- The FBI blew me off.
- I wrote a magazine column about the experience.
- Three months later, the Director of the Minneapolis FBI office read the article, called me, and wanted to troubleshoot.

# 2008 Norm Coleman for Senate Campaign.

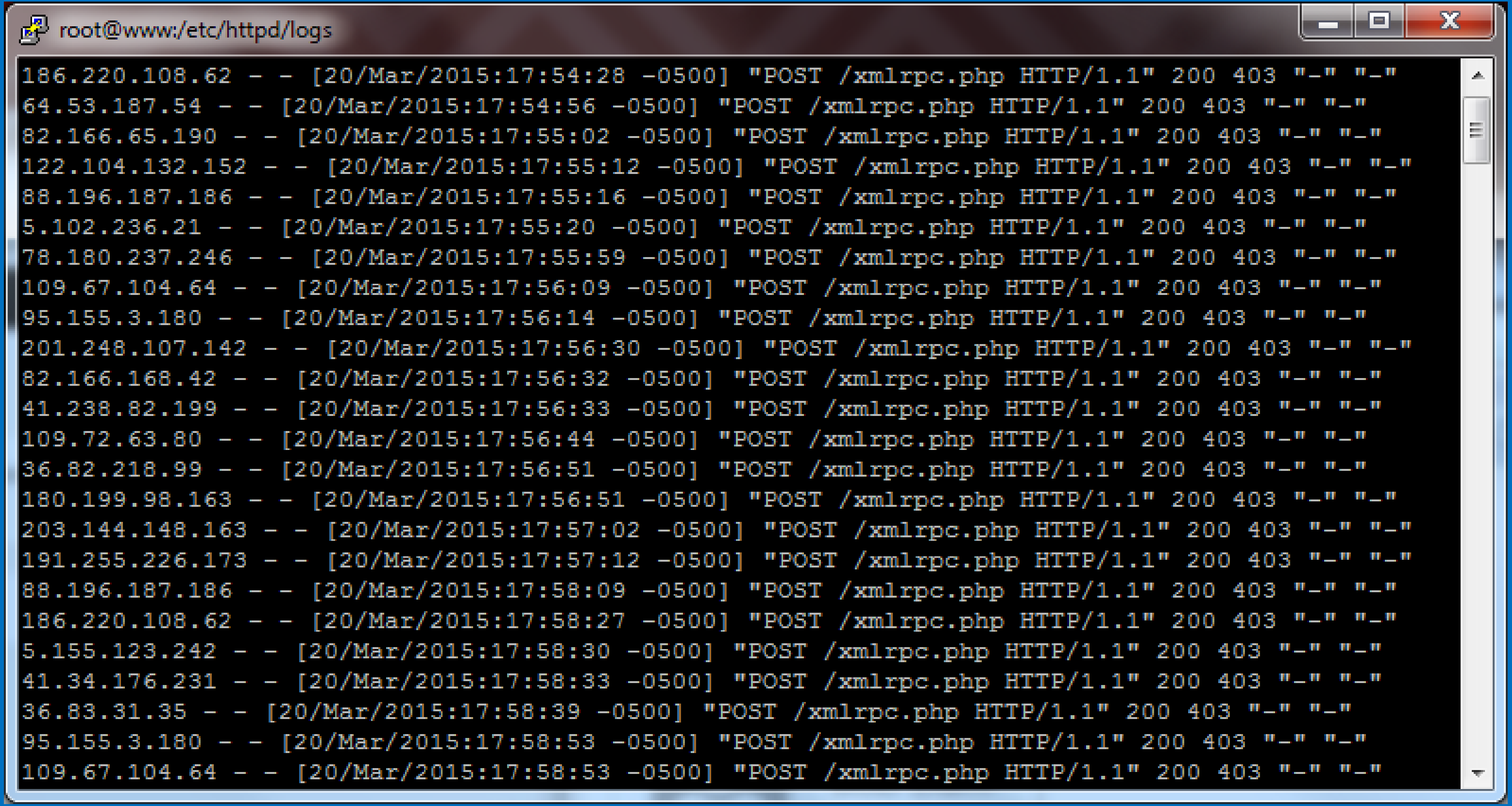
- Details here: http://www.infrasupport.com/gross-security-lapse-hurt-us-senate-campaign/
- I signed up to receive updates from the Minnesota Coleman for Senate campaign.
- Made me feel like an insider.
- March, 2009, I received an email from Wikileaks that my contact information was in a spreadsheet sitting on the Coleman webserver, wide open to the world.
- Fortunately for me, I never gave the campaign my credit card number.
- Others did and a few ended up as credit card fraud victims.

# Dec. 1, 2011 attempted credit card fraud

- Nov. 30, 2011 – I talked to Kim with the US Bank Fraud Department.
- We found these charges on my credit card:
  - Big Fish on 11/24/2011 at 2:20 PM Central time for $1.  Declined because the expiration date was wrong.
  - From Bayho, an online vitamin company:
    - 11/28/2011 10:47 AM Central time $3112.10 charged and reversed
    - 11/28/2011 10:50 AM Central time $6732.06 charged and reversed
    - 11/28/2011 10:52 AM Central time $4929.76 charged and declined
- Kim and I called the merchants and recorded names, dates, and transaction IDs.
- I packaged it all and sent it to a contact at the FBI.
- We traded a few emails and then…..
- I’m still waiting

# Recent attack on the *Bullseye Breach* website

- Looks like it was a brute force or dictionary password attack.
- IP Addresses from around the world – probably a botnet controlled by somebody like Bahir Mustafa.



```
186.220.108.62 - - [20/Mar/2015:17:54:28 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
64.53.187.54 - - [20/Mar/2015:17:54:56 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
82.166.65.190 - - [20/Mar/2015:17:55:02 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
122.104.132.152 - - [20/Mar/2015:17:55:12 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
88.196.187.186 - - [20/Mar/2015:17:55:16 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
5.102.236.21 - - [20/Mar/2015:17:55:20 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
78.180.237.246 - - [20/Mar/2015:17:55:59 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
109.67.104.64 - - [20/Mar/2015:17:56:09 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
95.155.3.180 - - [20/Mar/2015:17:56:14 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
201.248.107.142 - - [20/Mar/2015:17:56:30 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
82.166.168.42 - - [20/Mar/2015:17:56:32 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
41.238.82.199 - - [20/Mar/2015:17:56:33 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
109.72.63.80 - - [20/Mar/2015:17:56:44 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
36.82.218.99 - - [20/Mar/2015:17:56:51 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
180.199.98.163 - - [20/Mar/2015:17:56:51 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
203.144.148.163 - - [20/Mar/2015:17:57:02 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
191.255.226.173 - - [20/Mar/2015:17:57:12 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
88.196.187.186 - - [20/Mar/2015:17:58:09 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
186.220.108.62 - - [20/Mar/2015:17:58:27 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
5.155.123.242 - - [20/Mar/2015:17:58:30 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
41.34.176.231 - - [20/Mar/2015:17:58:33 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
36.83.31.35 - - [20/Mar/2015:17:58:39 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
95.155.3.180 - - [20/Mar/2015:17:58:53 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
109.67.104.64 - - [20/Mar/2015:17:58:53 -0500] "POST /xmlrpc.php HTTP/1.1" 200 403 "-" "-"
```

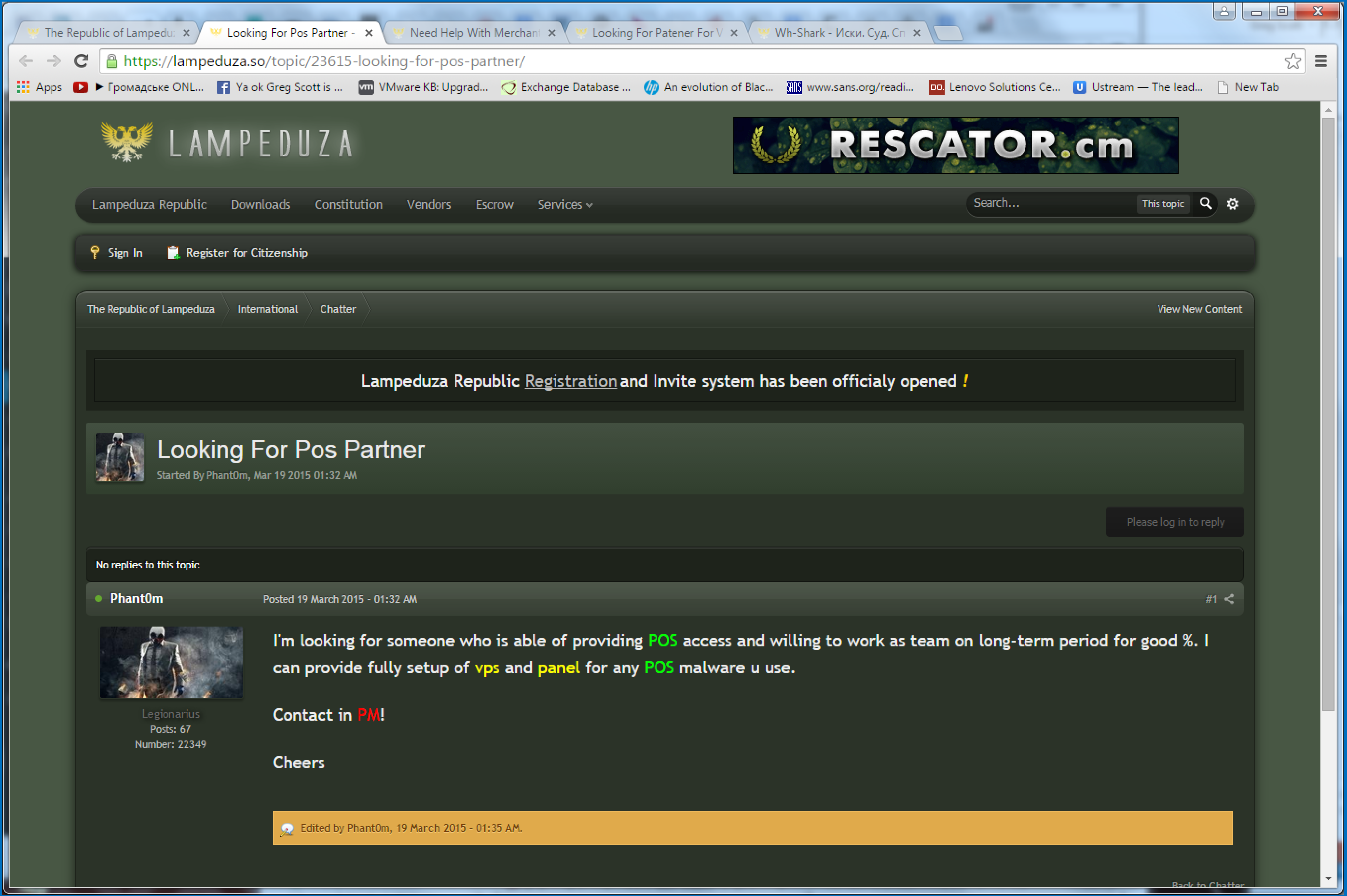
# Time to recap – what are we up against?

- Bad guys have a vast underground supply chain and support network.
- The companies we're supposed to trust with the Internet security infrastructure have all been compromised.
- At least one major credit reporting agency sold our personal information to an illegal identity theft service.
- Thousands of businesses have been compromised.
- Our own government is both a perpetrator and a victim.
- If your identity is stolen, law enforcement is unwilling or unable to help.

# How?

- How do 2-bit sleazebags plunder our Government and Fortune 500 companies seemingly at will?

- And why do business leaders and politicians keep hiding behind weenie excuses?



Lampeduza Republic Registration and Invite system has been officialy opened !

Looking For Pos Partner

Started By Phant0m, Mar 19 2015 01:32 AM

No replies to this topic

Phant0m Posted 19 March 2015 - 01:32 AM

Legionarius
Posts: 67
Number: 22349

I'm looking for someone who is able of providing POS access and willing to work as team on long-term period for good %. I can provide fully setup of vps and panel for any POS malware u use.

Contact in PM!

Cheers

Edited by Phant0m, 19 March 2015 - 01:35 AM.

# How do bad guys win?

# They collaborate.

# What do we do about it?

Buy a cave in Montana and hide.

Pay with cash.

Bad guys have unlimited time and creativity.

You don’t!

# Since hiding in a cave isn’t an option, what else can we do?

## Care!!

Teach CEOs and CIOs to listen to the warnings from your security team.

If your Chief Security Officer is an intern in the basement, upgrade the position.

**Message to CEOs:**

Pay more than lip service to taking security seriously.

Or look forward to lots of media exposure after the next breach.

# Share

- Bad guys already collaborate.  Why not level the playing field?

## Which do you prefer?

- Embarrassment during peer reviews with other good guys?
- Embarrassment in front of the whole world after 2-bit crooks plunder you?

# Layers of Defense

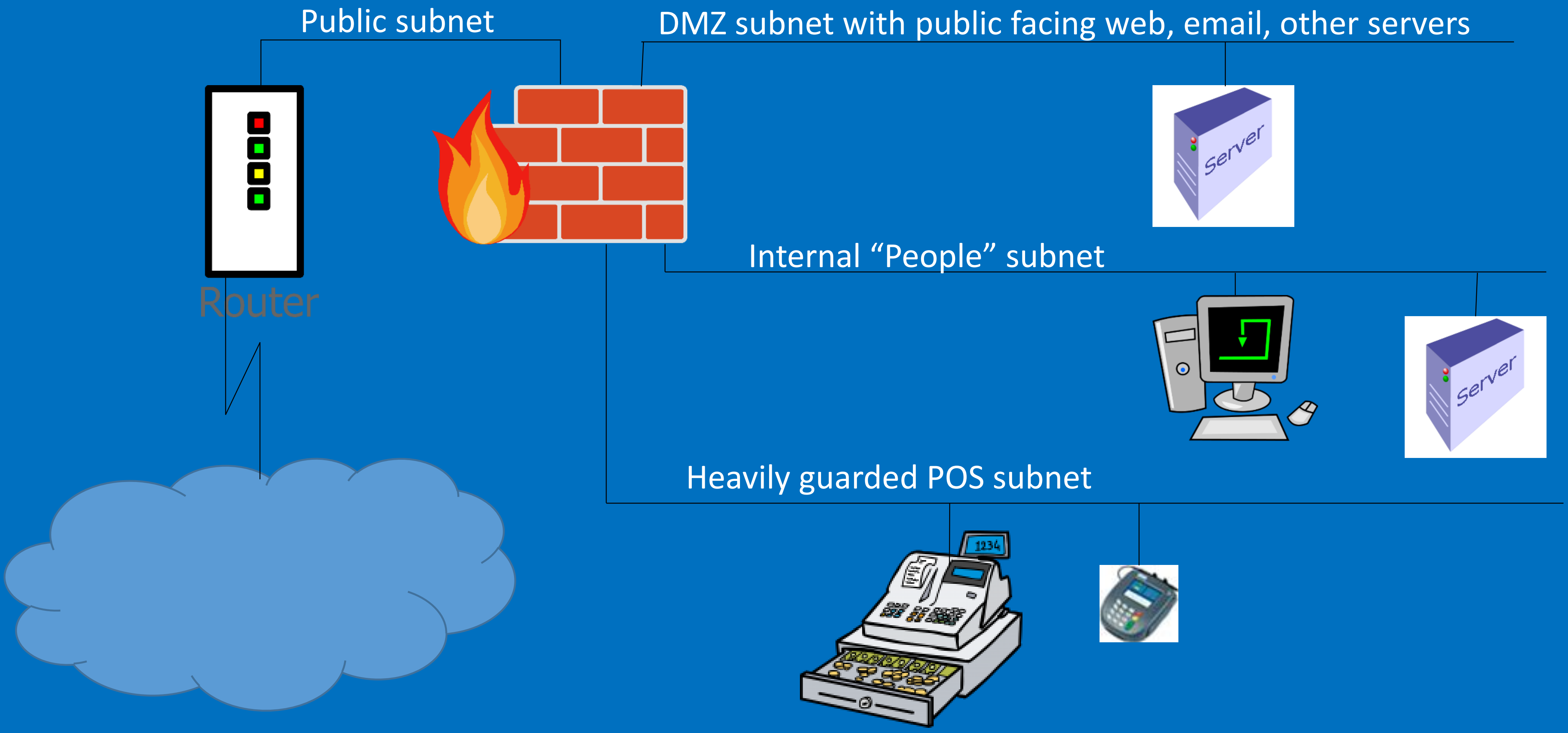
- Firewall(s)
- Antivirus subscriptions.
- Inbound email filtering.
- Outbound web filtering.
- Least privilege
- Traveling systems protected with filtering and personal firewalls
- Patching
- Educated and alert end users

# Software Defined Perimeter

- For less than $500 in hardware cost . . .
- Get a box with 5 gb NIC ports, 2 MB RAM, and a small SSD
- Build a basic firewall with Embedded RHEL or Fedora and an iptables script.
- Add Libreswan and/or OpenVPN connect branch sites and road warriors.
- Add snort for IDS.
- Add mrtg for historical trend analysis.
- Use tools such as iptraf and tcpdump for detail and debugging.
- Deploy two systems as an HA failover set with Gluster, or . . .
- Deploy as a virtual machine in a RHEV or other virtualized environment.
- Engage the creativity of the open source community for more.

# What’s your patching strategy?

# Topology counts


Public subnet
DMZ subnet with public facing web, email, other servers
Server
Router
Internal “People” subnet
Server
Heavily guarded POS subnet
1234

# Vigilance Counts

- Educate yourselves and your employees.
- Learn how bad guys think.
- “Just cuz you’re paranoid doesn’t mean they’re not out to get’cha!”

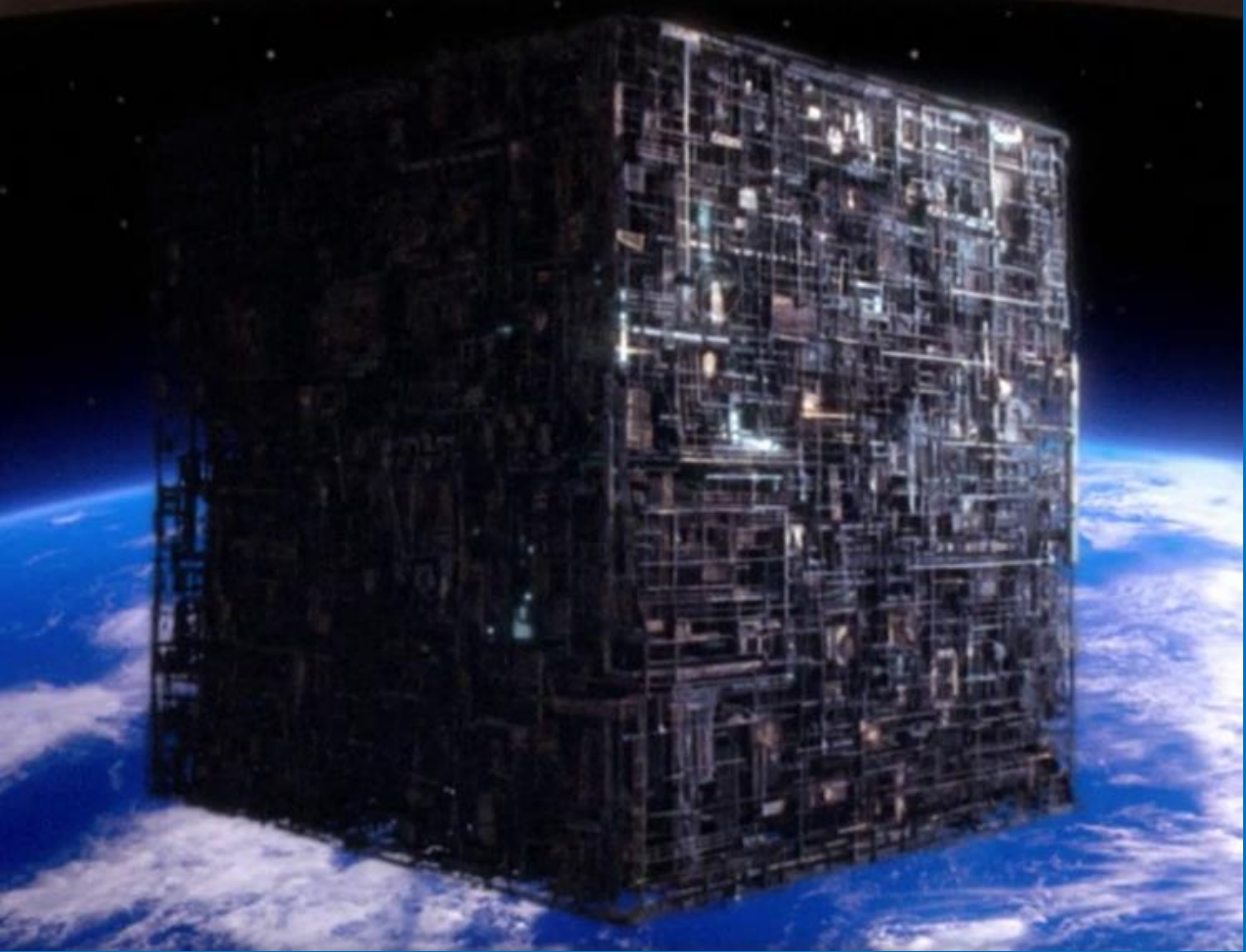
- If somebody calls from India and wants to do tech support on your computer…?
- If you see an email claiming to come from your boss with instructions to wire transfer $1 million to an overseas bank account …?
- If you see a solicitation for free (beer, porn, screensavers, Viagra, you name it), …?

# Security is a process, not an event

- Share what you learn with other good guys.
- ~~Expect~~ Demand other good guys share what they learn with you.

- Apply what you learn; repeat and refine continuously.

**Security is a process, not an event.**



Resistance
is not futile.

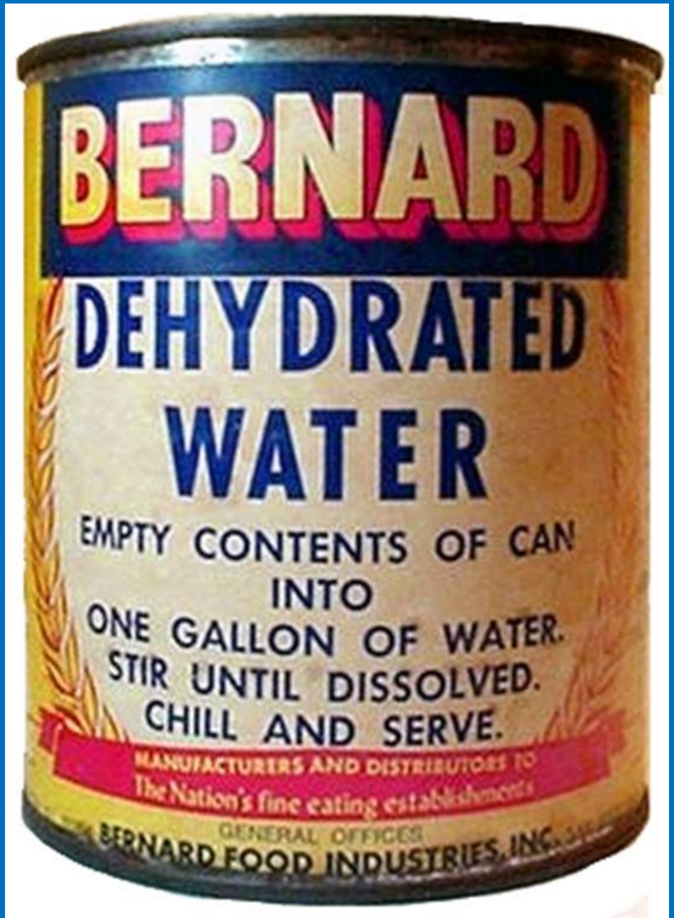
# A few references

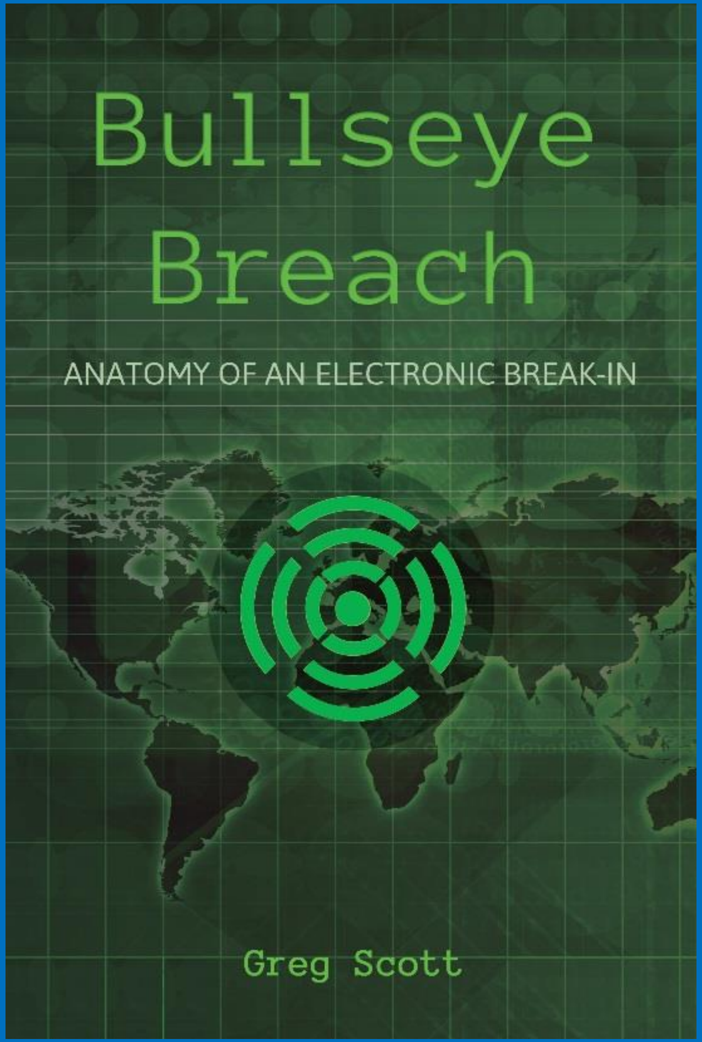
- Pretty much any article from http://www.krebsonsecurity.com
- http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data
- http://www.infrasupport.com/take-privacy-seriously-really/
- Network Security, Charlie Kaufman, Radia Perlman, Mike Speciner, Second Edition, Prentice Hall, 2002
- Building Internet Firewalls 2nd Edition, Elizabeth D. Zwicky, Simon Cooper, and D. Brent Chapman, O'Reilly, 2000.
- Linux Firewalls, Second Edition, Robert L. Ziegler, New Riders, 2001 for a general discussion on how to model TCP/IP conversations.

# Some really good reading

- http://www.infrasupport.com/spying-the-pot-calling-the-kettle-black/
- “Countdown to Zero Day,” Kim Zetter, Crown, 2014.
- “Spam Nation”, Brian Krebs, Sourcebooks, 2014
- Hacking Exposed, Joel Scambray, Stuart McClure, and George Kurtz, Osborne/McGraw-Hill, 2001.
- Takedown, Tsutomo Shimomura with John Markoff, Hyperion, 1996
- The Cuckoo’s Egg, Cliff Stoll, Pocket Books, 1990

# Con games are alive and well today and live on the Internet





# Contact info

Greg Scott

gregscott@infrasupport.com
Twitter: DGregScott
http://www.bullseyebreach.com

+1 (651) 260-1051

(And watch for book #2, coming soon. What happens when a nation-state really does launch a cyber-attack against the United States?)