Cops and Admins
15 years later

SysAdmin Campfire Stories

usenix LISA15
November 8–13, 2015 | Washington, D.C.
www.usenix.org/lisa15 #lisa15
Tom Perrine
Sony Computer Entertainment



usenix
LISA15

Set the wayback machine



Cops are from Mars, SysAdmins are from Pluto

Tom Perrine

tep@sdsc.edu

SAN DIEGO SUPERCOMPUTER CENTER

A National Laboratory for Computational Science & Engineering

usenix LISA15

At some point, you will need a little help

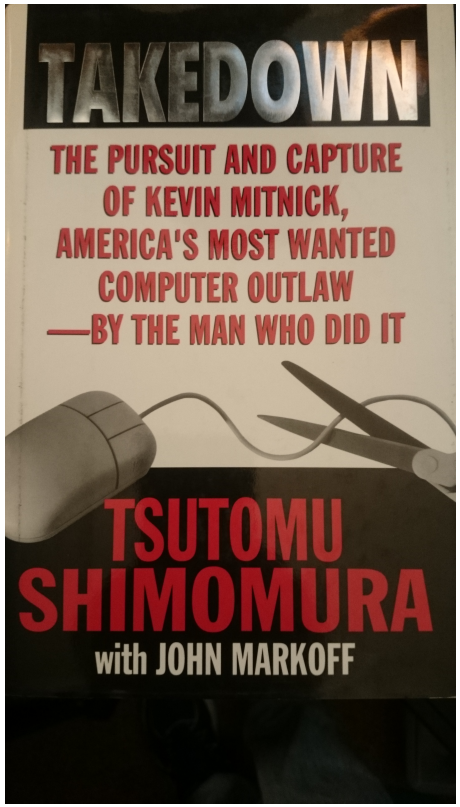


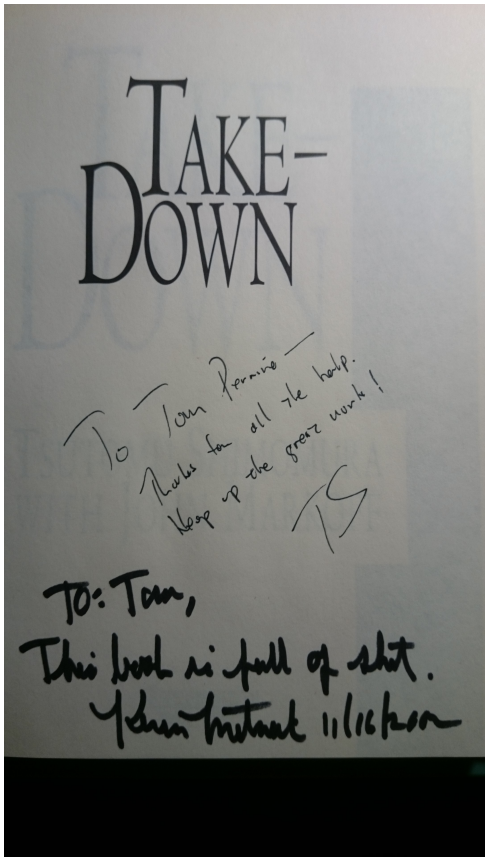
The Rules

- Never talk about active cases
- Always protect sources and methods
- Always get competent legal guidance
- I don’t speak for any current or former employer, I’ve never been a lawyer



A long time ago there were these guys





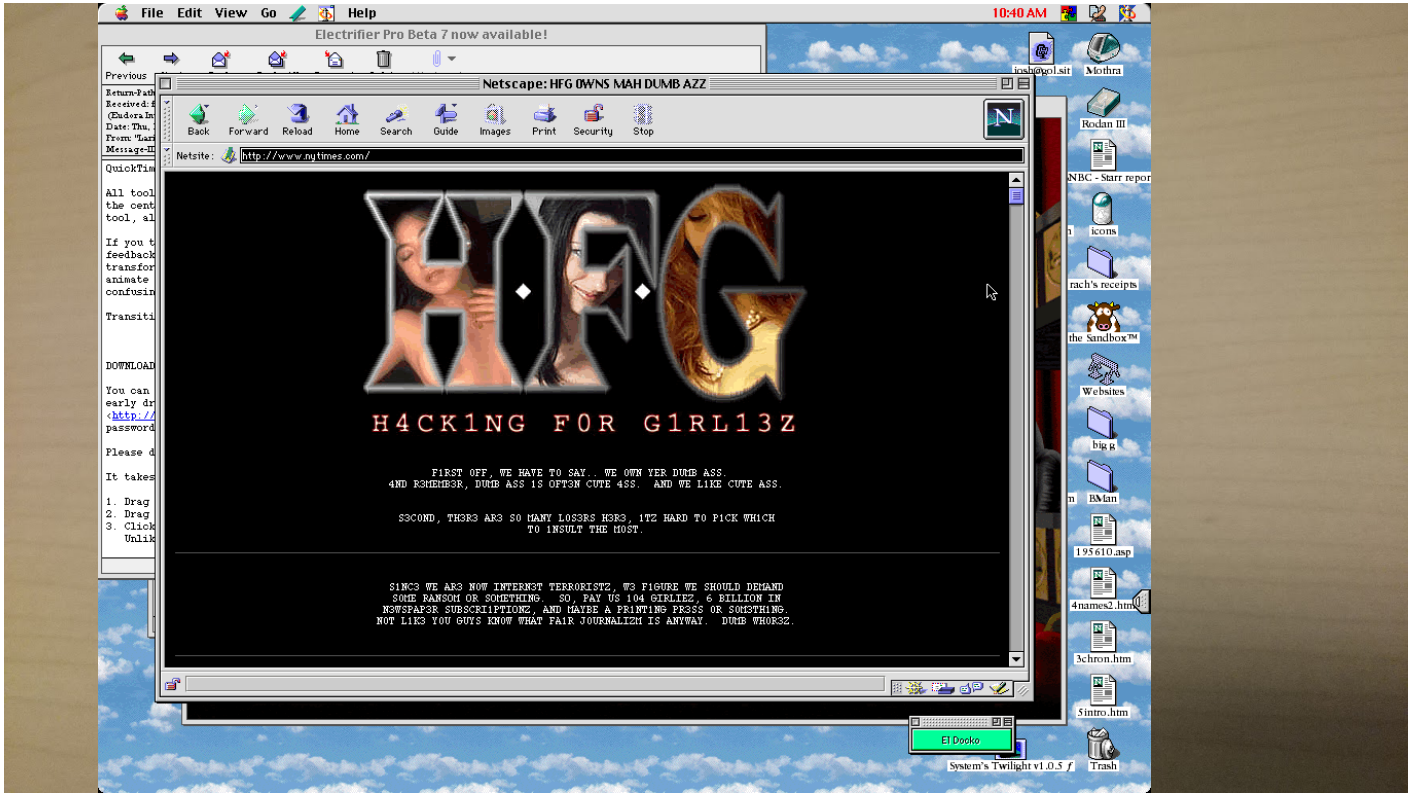
Secret Service Agent Stevens




DEF CON III
Las Vegas 1995 Las Vegas 1995 Las Vegas 1995 Las


Phone

H4Ck1NG F0R G1RL13Z



usenix LISA15

ICAC
Internet Crimes Against Children
Task Force





INTERPOL

usenix
LISA15

Decide who to trust, and when

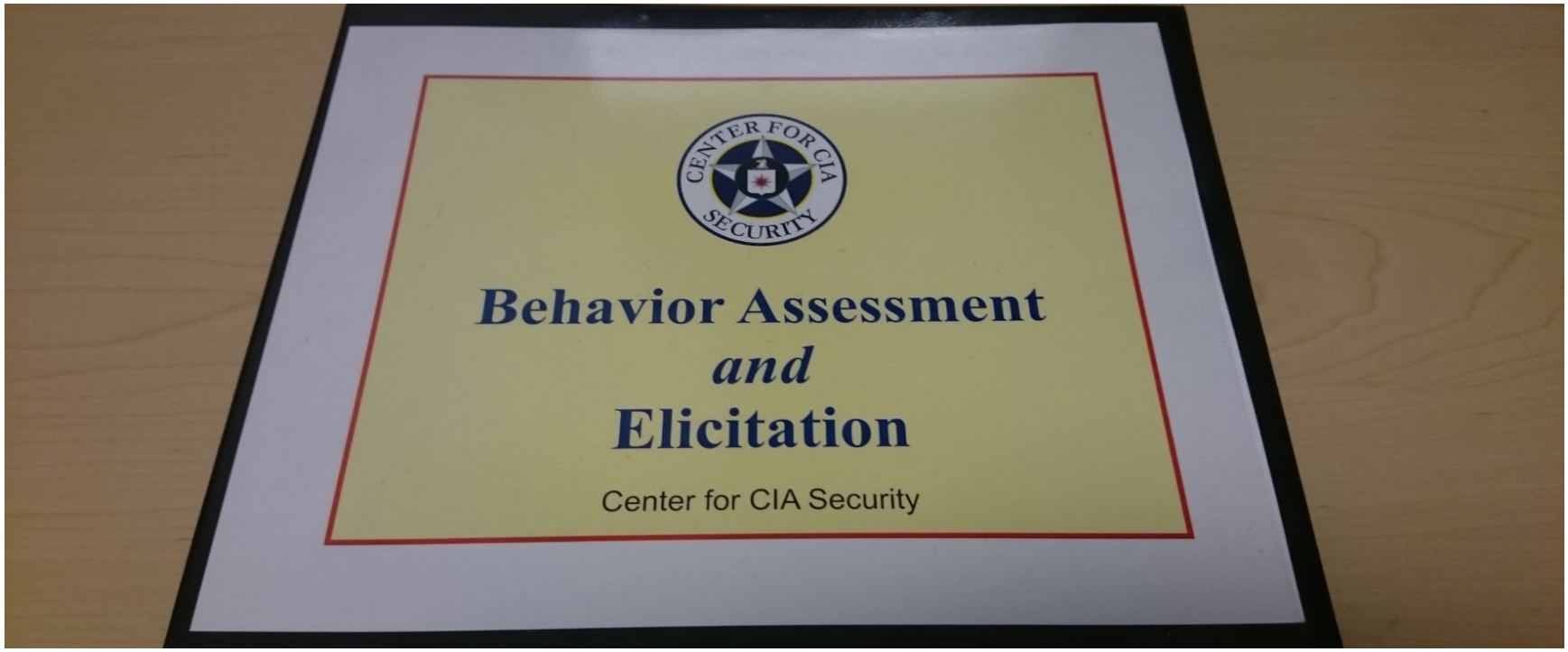





High Technology Crime Investigation Association
HTCIA
1986-2007


REGIONAL COMPUTER FORENSICS LABORATORY
SAN DIEGO


INFRAGARD
PARTNERSHIP FOR PROTECTION


CENTER FOR CIA SECURITY
Behavior Assessment
and
Elicitation
Center for CIA Security

Be willing to help









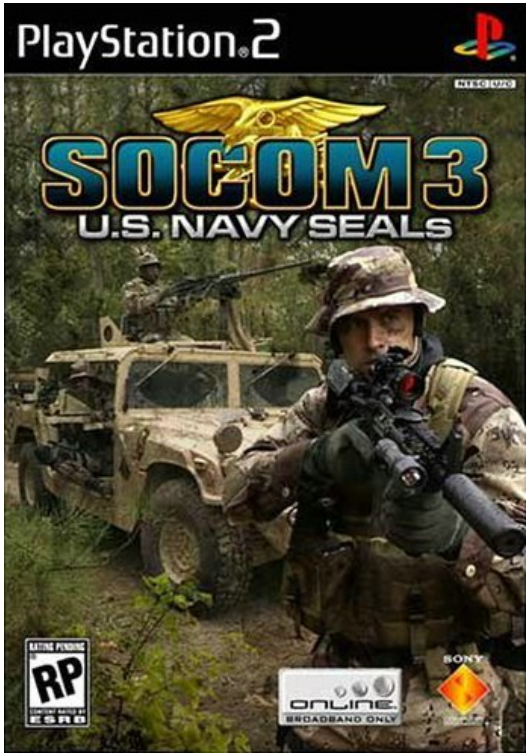
- Threats against schools
- DDoS (many)
- Online bomb threats



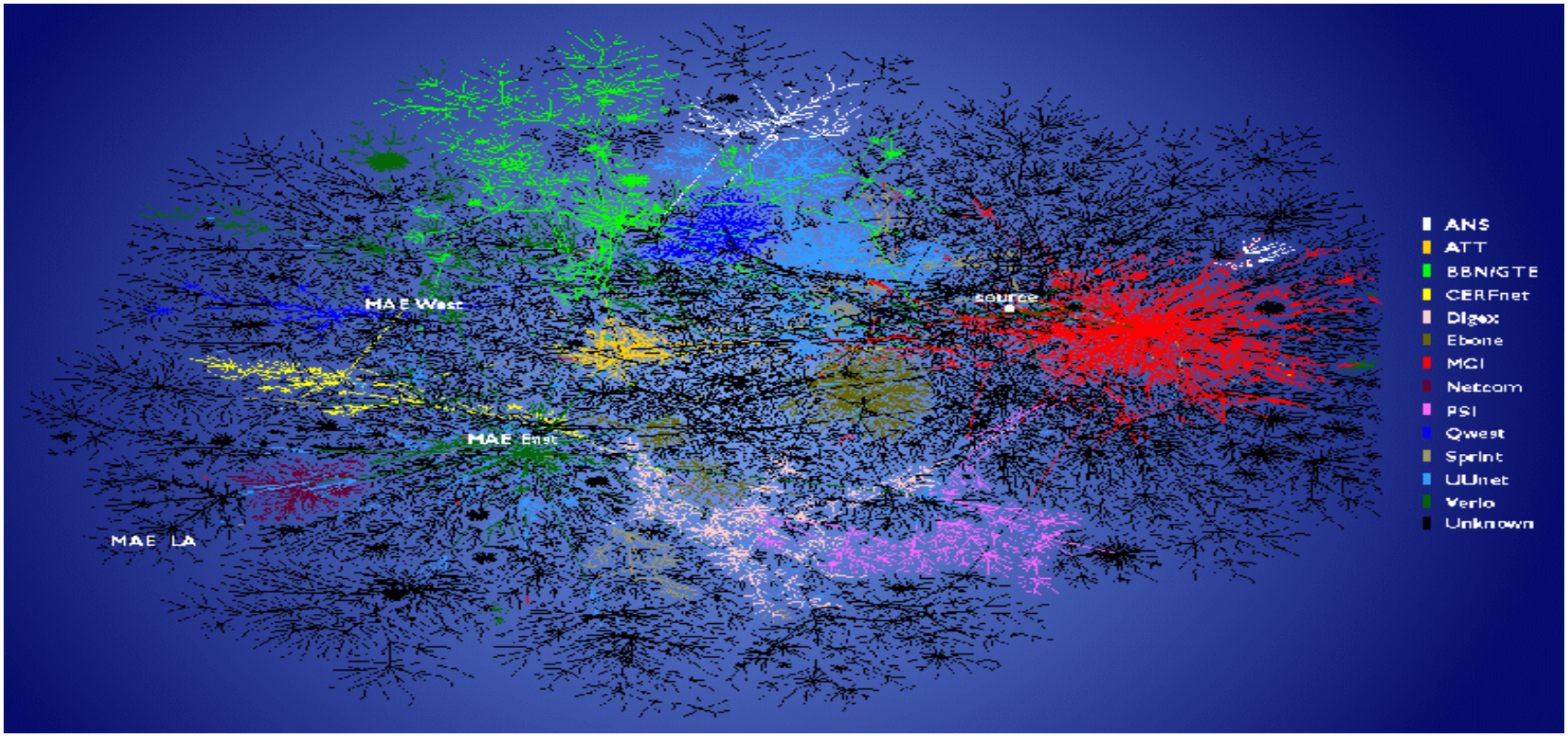
- Recovered intellectual property
- Early warnings for some attacks
- Assistance with death threats to our staff

SOCOM DDoS


PlayStation.2
NTSC U/C
SOCOM II
U.S. NAVY SEALS
MATURE 17+
M
CONTENT RATED BY ESRB
ONLINE
BROADBAND ONLY
SONY


PlayStation.2
SOCOM 3
U.S. NAVY SEALS
RP
ONLINE
BROADBAND ONLY
SONY

Online Games



February, 2008

NOC: “We just dropped a bunch of players…”

“Hey, one, no, two of the S2 servers just crashed…”

“Wait, make that 5 servers. That’s weird. Never done that before”

“I wonder if it was that application update that was just applied?”

This goes on for several nights…

Log analysis and packet captures eventually show a IP fragment DDoS attack

But it stops before we can get a good handle on it…



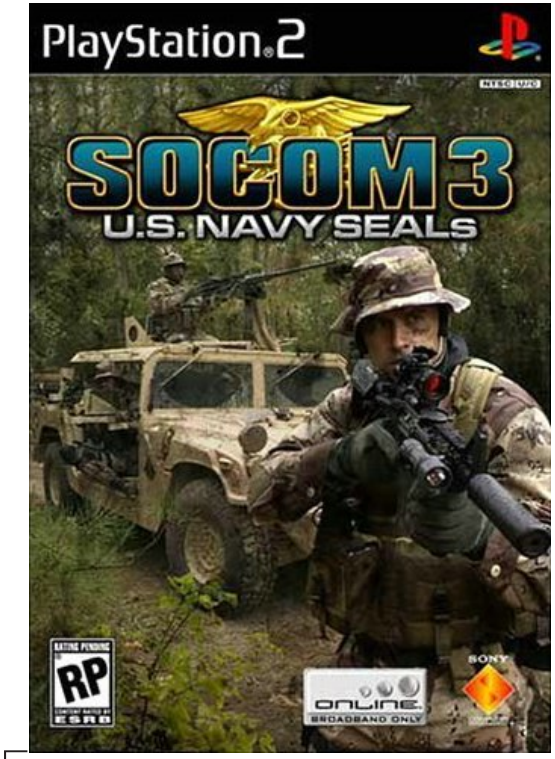
And then we got busy…







November, 2008



0300, when SysAdmins are asleep..

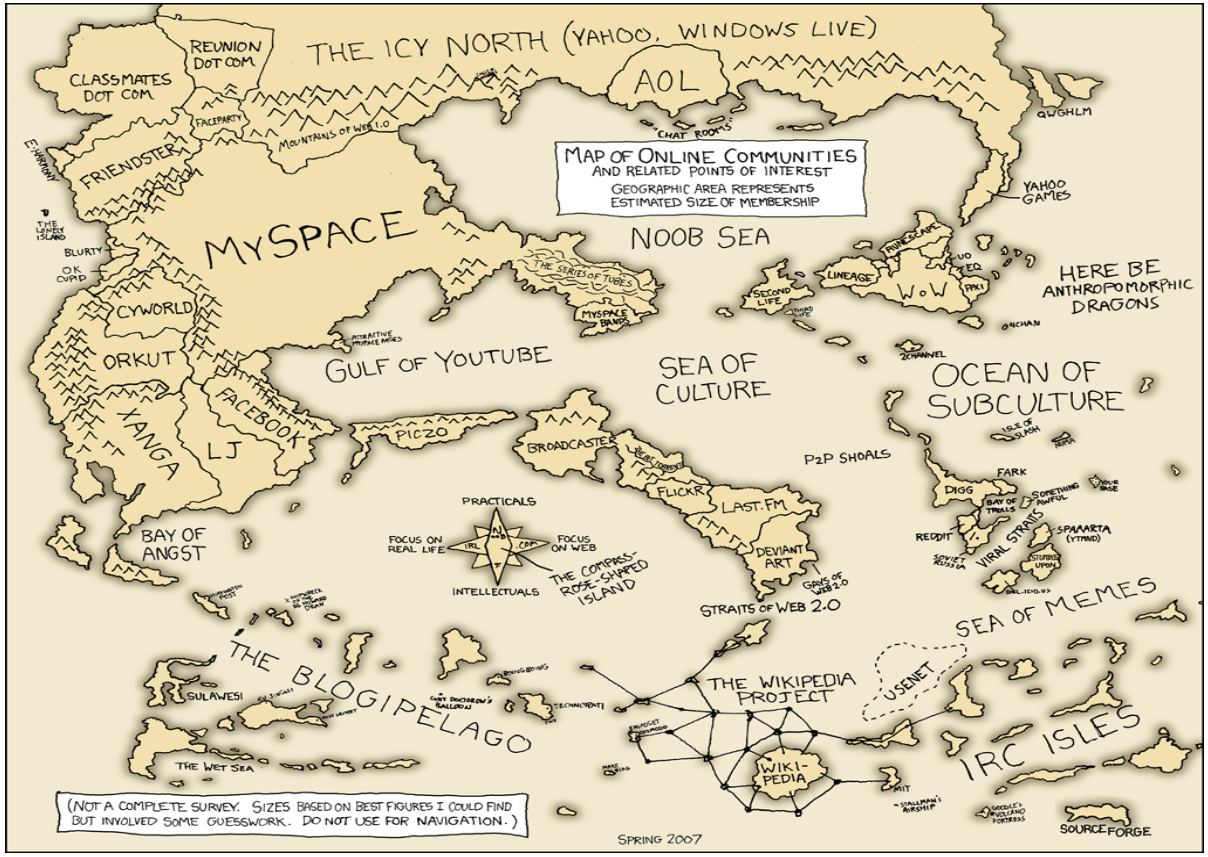
NOC: “We just dropped a bunch of players…”
“Hey, one, no, two of the Socom 3 servers just crashed…”
“Wait, make that 8 servers. That’s weird. Never done that before. OLS can’t get back in, either.”
“I wonder if it was that application update that was just applied?”

“Let’s call the SysAdmins…”

Ruh, roh….



But, where is it coming from?

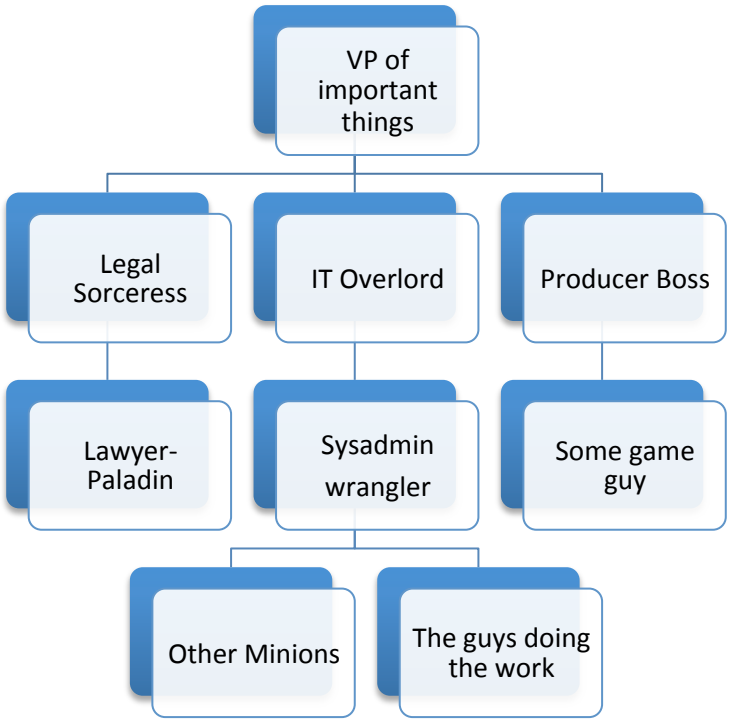


usenix LISA15

How cute, it’s a baby botnet



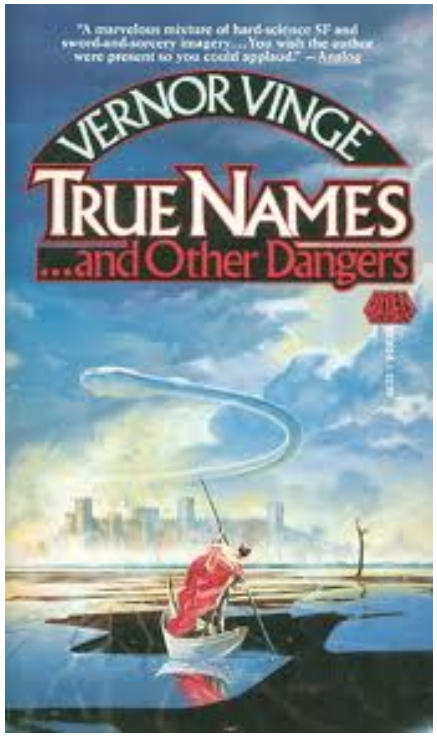
Meanwhile, in Management Land



Something wonderful is about to happen…



True Name == Leverage



- We have nickname(s), IP addresses and timestamps
- We trace the primary suspect ("ADMIN-ANGEL") to an ISP in PA
- Social networking sites can provide a wealth of information
- We have "True names" + city/state for primary and two other suspects

(ADMIN-ANGEL, neo-2-remember and one more)

ADMIN-ANGEL in our sights…



- Attack timing
- Block home IP addresses
- Attacks taper off after we "kick" him
- No attacks if he can't get in
- and finally… bragging in voice chat…

Shutdown -h

With Legal's OK, we contact the ISP and escalate to their security team immediately



We want additional confirmation so….

- We will wait for the next attack, and the ISP will disconnect service during the attack for violating their TOS

2 PM Sunday (23 Nov 2008)

- Attack begins
- Legal, ISP security and our IT on a conference call
- We provide the current IP
- ISP suspends service (2 cable modems. Wait! What?)
- New attacks stop
- Current attacks fade away (as botnet hosts are presumably turned off or rebooted by owners)

Monday

Our first FBI meeting

We provide DVDs with:

- 18 G of log data
- 18 pages of timeline and incident log notes (at 10pt type, single spaced)
- Emails and trouble tickets

Screenshots of social networking sites for all three suspects



"By the time the interview came, [the] victim had gift-wrapped the attacker for us
We left the initial meeting with enough probable cause to start work on the warrant [which is almost unheard of]" - FBI

Well, that was fun….

At the end of the week, no new attacks

Looks like we got him?

But, you just know what is coming…




ITS QUIET
Too quiet.

Through December 2008

- SYN floods are pretty much stopped dead
  - But “ADMIN-ANGEL” is back in game
- Then the attack profile changes from SYN flood to IP fragmentation attack
- Re-load the IP frag defenses….



January, February 2009

- Attack moves to application level
  - Developers find and fix
- Attack profile changes again – targets load balanced servers
- Then, in February, nothing…



March 2009

Attacks begin again…



The attacker is bragging to his friends online

Then, a phone call from the FBI…

"ADMIN-ANGEL has been arrested at his High School. We seized computers, game consoles, game discs, everything"

April – August 2009

- Attacks continue, and finally taper off
  - Identical to prior attacks, nothing new
  - Mostly when two secondary suspects are online
  - Attacks become ineffective as we increase countermeasures

- FBI begins to ask questions, based on information in suspect's seized equipment

September - December 2009

- Ineffective attacks continue and finally stop after primary suspect is re-interviewed by FBI and local Sheriff

- more meetings with FBI/RCFL to discuss forensics on seized computers

March 2010

After being charged with 15 felony counts, plea bargain discussions begin

- After all is said and done, juvenile suspect “ADMIN-ANGEL” pleads guilty to 5 felonies
- Juvenile is “adjudicated delinquent” and sentenced

In PA, juvenile felony convictions are not sealed


FIN

August 2012

Suspect #2 (neo-2-remember) is arrested in Columbus OH

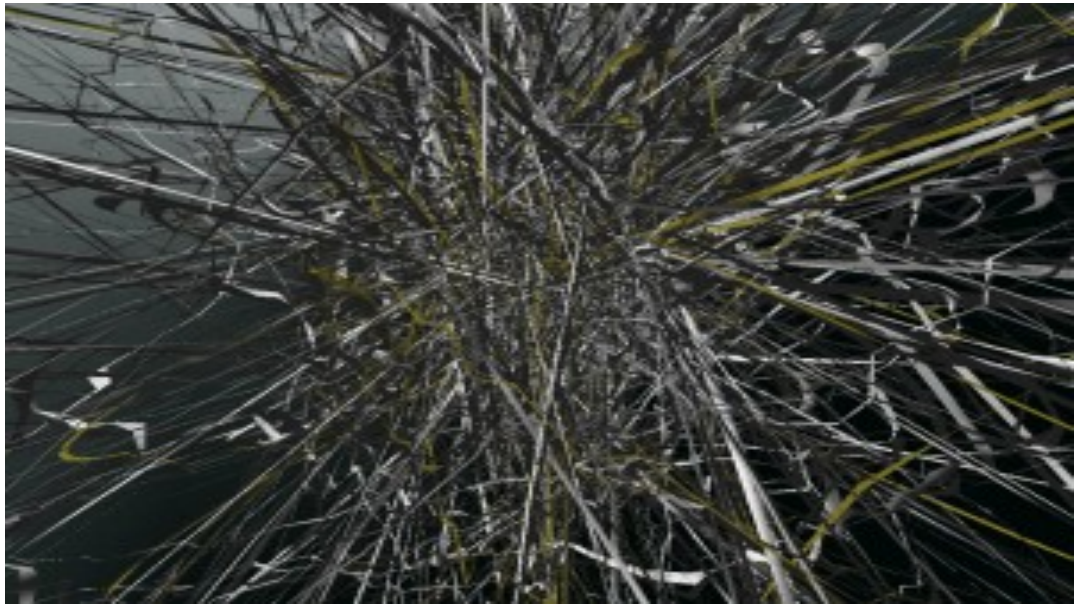
- He's an adult – will be charged in Federal Court
- Multiple computers, consoles, media seized
- He and his father are involved with other (non-computer) criminal activities



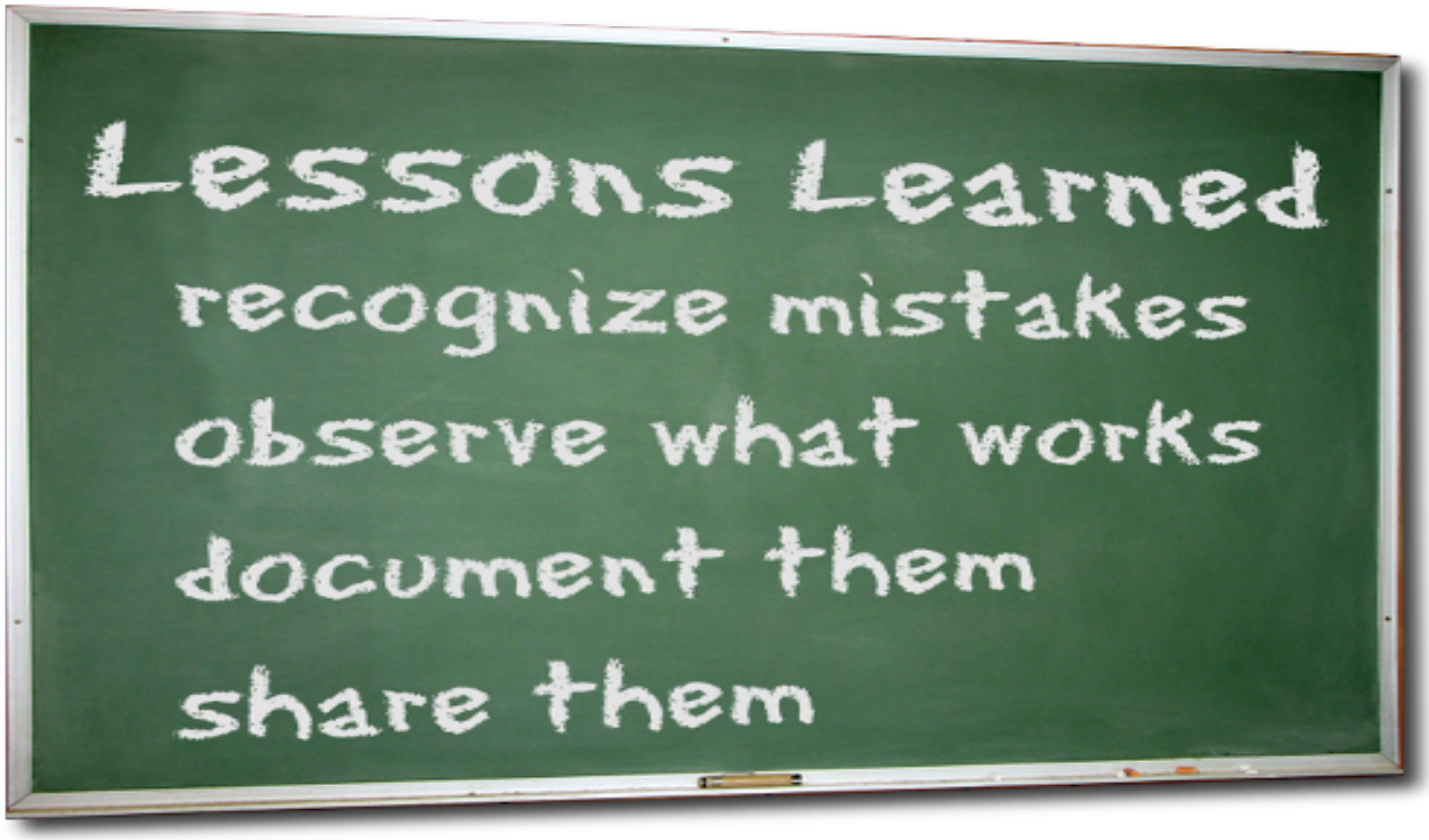
Summer 2013

- Neo-2-remember pleads guilty to felonies
- Father convicted on CP charges

Is it all over, finally?



Our case spawned at least 5 other cases over the past years


Lessons Learned
recognize mistakes
observe what works
document them
share them

Relationships matter

- Relationships matter – have a personal web of mutual trust
  - Know who to trust (people, not organizations)
  - Know who you may need and who may need you
  - You want to call Tier-3, not Tier-1
  - Play the long game
- Build the relationships today that you will need in the future
- Help others, and they will help you

Have a plan

- Know your goals – they may not be the same as law enforcement or other related victims
- Build those relationships now; when you need them is too late
- Know your limitations – legal, technical, business, financial

Know your Criteria for Success

“fighting for our gamers”



Management support
- Trust, patience, encouragement, room to maneuver

Legal support
- Trust, flexibility

Technical team
- Skills, teamwork, determination, sense of ownership

“There is a positive correlation to how well your IT staff handles the incident to how well the investigation goes.” – FBI incident report

SOCOM DDoS plan (2008)

1. Preserve the customer experience

2. Improve security and tools across the board
   - Engineer a solution for *this* particular threat while also creating solutions for the future

3. Collect information to preserve options
   - You're doing it anyway as part of incident response, Prosecution may be viable

4. Contribute to the community**
   - So that others may learn from our experience

Remain Independent

- Never become an agent of the government
- Remain focused on your goals
- Your goals are not their goals

Be patient

- Investigations take months
- Cases take years

- Not all cases will get government resources

- Many cases will go nowhere on their own, but some may lead to other, more serious cases and people

You never know where a case will lead



Be kind

- Have empathy for other victims and your fellow admins
- Everyone is doing the best they can under the pressure

More than just hacking



One suspect may have been involved in making pipe bombs

Another made death threats against the President



Evidence

- ***Log like you mean it***
- Learn at least a little about chain-of-custody for evidence
- Logs and remote digital evidence usually leads to digital evidence on a suspect's equipment, and then to physical evidence
- physical evidence is easier for a jury to understand

Truth

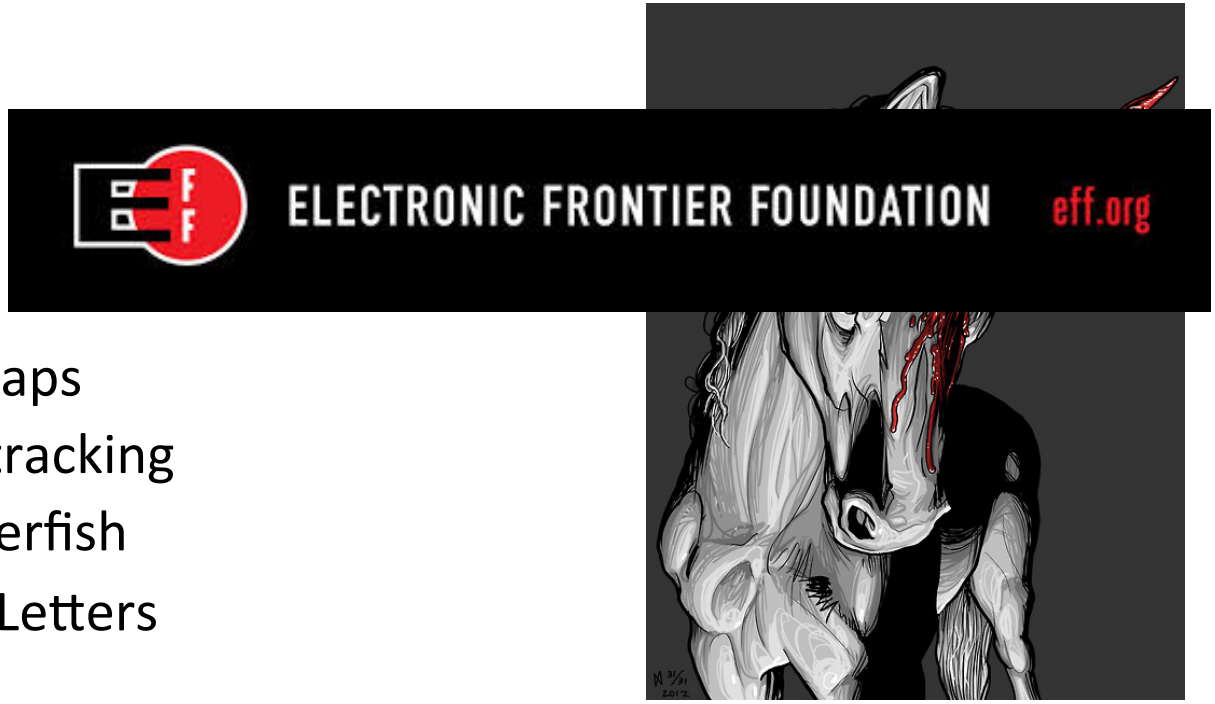
- Three books and a movie can all be made from the same case, and have no agreement and little basis in reality

- “Logs or it didn’t happen”

- Truth is what you can prove in court
- Truth is what you can help a jury understand

It's not all Unicorns and Rainbows

- PATRIOT
- PATRIOT II
- PRISM++
- XKeyScore
- Warrantless wiretaps
- Warrantless GPS tracking
- Warrantless Triggerfish
- National Security Letters
- FISA Court



Lessons for Management

- “bad things” are going happen
- Everyone will be doing the best they can, give them room, don’t panic, and Listen
- Be available

Credits

- World Wide Studios IT staff (esp. “hockeygeek”, “Mac”, Ian, Steve-o)
- WWS Online Services
- WWS Management
- SCEA Legal

- FBI “TR”, “Amanda”, “Todd”, William Gore
- AUSA Mitch (“Dr No”) Dembin, San Diego Grand Jury
- “Tim” at RCFL

- Andrew Gross
- Tsutomu Shimomura
- SDSC IT staff, esp Jeff Makey
- Dr. Sid Karin

- PA ISP Legal and Security teams
- Sheriff’s Office and ADA, Westmoreland PA