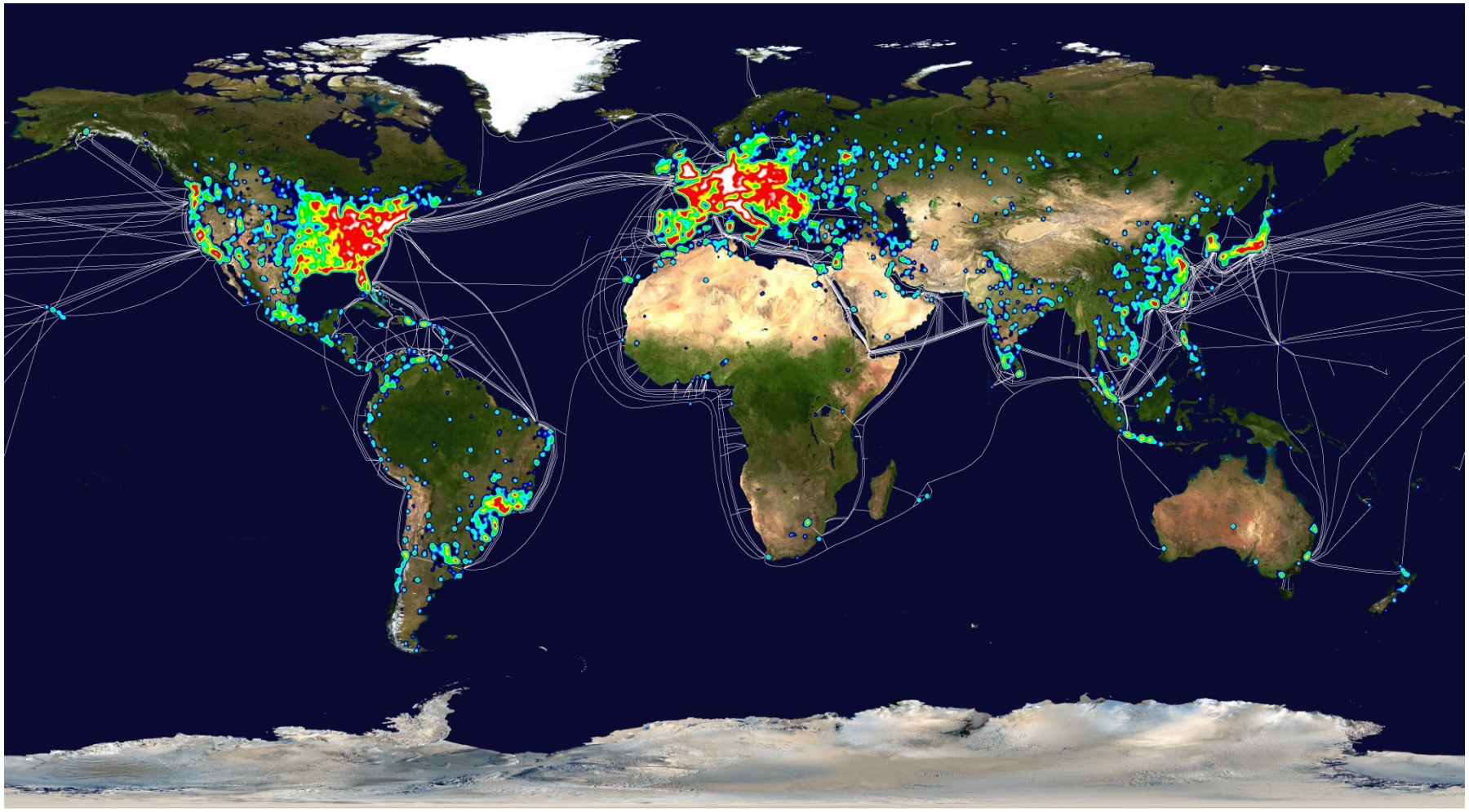
The Dark side of the Net or "Why Internet Security S*x!"

John Kristoff jtk@cymru.com
jtk@depaul.edu

Malware to submarine cables



$$$ MAKE MONEY FAST $$$

<A> i have access to accounts ranging from a few hundred thousand to several million that i have the ability to wire from

<A> but i've been talking to people high up in banking and they've basically told me no wire above $50,000 will probably go through so i'd be looking at wiring below that amount

Welcome to the underground


```
< Ba
 in
  ww
  ms
< PaypaLKinG>  Buying: fresh or normaL 9-10 cc
* Idol I am Selling Shopadmin with 800 paypal there - USA, UK and
  International Shopadmin - Egold Only
* ScreeN Need Legal Shell Stable..! MSG ME!
-!- ipod100gb [ipod100gb@ipod100gb.Users.RealUnix.Net] has joined #ccpower
< [freeMAN]> I SELL PHP MAILER SEND ALL INBOX (HOTMAIL-YAHOO-AOL)
 (7$) ,HACKED ROOT (15$) , HACKED HOST WHIT (FTP) F0R SPAM (5$) , FINDNOT
 ACCOUNT 6 MONTH (5$) , 10mb us fresh mail list only 50$ , SHELL (5$) ,
 PowerEmailVerify (4$) , SCAM PAGE+LEETRE for FREE
  http://younes.by.ru/scampage2007 /payment via egold
< christy> Selling Hacked Host Support Cpanel+FTP, PhPMILLER SEND
 ALL INBOX, Cvv2 Us/Uk All Country, Paypal Verified, r57/c99 Phpshell,
 Citibank Login, Pm mE foR dEal !!!
< intel>  sell hack host cpanel+ftp acces, cvv2 (US and UK) pay via e-gold
```

xone2014@yahoo.com	Perfect Keylogger report: 2/27/2007, 8:38 AM (FLD-GOVT-GM\zakaryan)	Tue Feb 27, 2007	29k
xone2014@yahoo.com	Perfect Keylogger report: 2/27/2007, 8:07 AM (FLD-GOVT-GM\zakaryan)	Tue Feb 27, 2007	12k
xone2014@yahoo.com	Perfect Keylogger report: 2/26/2007, 11:36 PM (FLD-GOVT-GM\zakaryan)	Mon Feb 26, 2007	31k

Rent to pwn

<A> A "rented" skimming set is merely the same set but you do not get the Encryption key

<A> you send us the tracks immediately after getting them, we decode, cash out approx half

<A> the cost of the rental units are €900

<A> after 1 use, it is yours, as we will have made more than enough money to cover our costs

Then they come after us

<A> terminated [my VPS] because apparently someone was running “ddos tools” and “ssh scanners” on it

<A> Anyone got old ccs or hacked paypals

<A> To order heaps of @?#! from them, then ?!@# up their paypal with disputes

No firewall upgrade for this

- What IDS is going to detect it? Or even see it?
- Who do you call for help?
- Can you over-engineer around this problem?
- How will you know when you have a problem?
- Is this even a technical problem?
- Law enforcement challenges
- For miscreants, it is all about the bling-bling
- For us it is all about SIGINT, or maybe NETINT?

Interconnected, co-dependent, and mutual trust

- Interconnected
  - The whole idea of a network is to connect things together. Connectedness is its own reward.
- Co-dependent
  - No-one person or entity owns and operates all the pieces that make up all the interconnections
  - **Though some do try to grab as much as they can*
- Mutual trust
  - For endpoints to communicate, many autonomous pieces have to cooperate.

So who is in charge of security?

More interesting question... Who is responsible for the security we now have?

The free-love gray beards?

- The line
  - The no-shower-taking, pot-smoking, government-protesting, communist hippies forgot security when the Internet was built!
- Not exactly
  - Some gray beards wanted to include end-to-end encryption and an authentication infrastructure, ARPA apparently wouldn't fund it
  - Some “best practices”, as we'll see, and even government laws can restrict end-to-end security

The protocol designers?

- Example, “TCP/IP is full of security holes!”
- There are some weaknesses in some core protocols
- But...
  - We're still using much of the original design 25+ years later and the world hasn't ended yet, that's pretty good evidence they were well conceived
  - Implementation bugs or implementation short-cuts often underlie the real problem

The programmers?

- “Programmers are lazy!”
- Well, they are human
- But
  - Are programmers rewarded for bug-free code?
  - Are programmers taught secure coding practices?
  - Do languages and tools make it hard or easy to write secure code?

The schools and teachers?

- “Schools don't teach security”
- Historically, mostly true
- Encryption protocols usually get a lot of coverage
  - Its important, but plain text is a small part of the problem in the real world
  - Students lack good real-world experience
  - Most teachers lack it too
    - ** but none who do think so or would admit it :-)*
- How do you get experience and good mentors?

The silicon snake oil vendors?

- They sell band-aids, but we need an operation!
- How do you operate on one the most prolific distributed systems ever devised and implemented?
  - You don't, you hack and you hack and you hack
- Operators need to balance the hacks, the complexity, the cost, the risk, etc...

The ISPs?

- Why don't they just block this junk?!
- Some do, some can't, some will, sometimes it works
- What is “junk”?
  - If it is user-defined, how does a ISP deploy custom user-defined junk filters for thousands of customers? Things don't always “scale” so easily.
  - As new apps are deployed, new junk is invented
  - Where does protection stop and censorship begin?
  - A few angry users should not be underestimated

Can't we just blame Microsoft?

- Yes! Personally Windows 95 is on my s**t list
- But market share does attract attention
- You think UNIX systems haven't had gaping holes?
- The OS is much less the problem now
  - FINALLY!
- Too bad there are plenty of vulnerable apps!

Let's go back to mainframes?

- I think some people should
  - Security dilettantes especially
- And some should never touch a computer again
- But
  - Security wasn't always so great there either
  - Plus, that would be wicked lame!

Isn't C an insecure language?

- Or is that unsecure?
- In wrong hands, yes it can be dangerous
  - As can be Perl, javascript, C++, etc.
- It was thought Java would replace C/C++
  - All I have to say about that is.... BWAahahaha!
  - Widely deployed code can last practically forever
  - Note... I don't disable Java in my browser because I hate coffee

You, security dude, your fault?

- Yes, but maybe you didn't pay me enough
  - But it's really Sid's fault - **some .nl guy we can pick on*
- Personally
  - I think many security dudes make things worse
  - They mean well, but do long term damage
  - The more you hack, the harder a real fix is
- Consider
  - Where is security on the balance sheet?

What about the bad guys?

- Yep, they should be put through the spanking machine
- Dealing with the perps is a HUGE challenge
  - There are lots of bad actors out there
  - Bad events occur constantly (spam, theft, DDoS)
  - Who brings the case to law enforcement?
  - How do you map the crime to a jurisdiction?
  - What does evidence collection look like?
- Self-appointed groups (vigilantes?) sometimes help
  - But sometimes come with their own can of worms

Can't we legislate this away?

- Haha, been in the U.S. Long?
- Some government reps think the net is a toy
  - Or maybe a series of tubes for spreading rumors on the internets
- Some legislation might be helpful
- But perhaps
  - Some frequent and high-profile convictions might be a better deterrent
- Then again, how do you police the entire world?

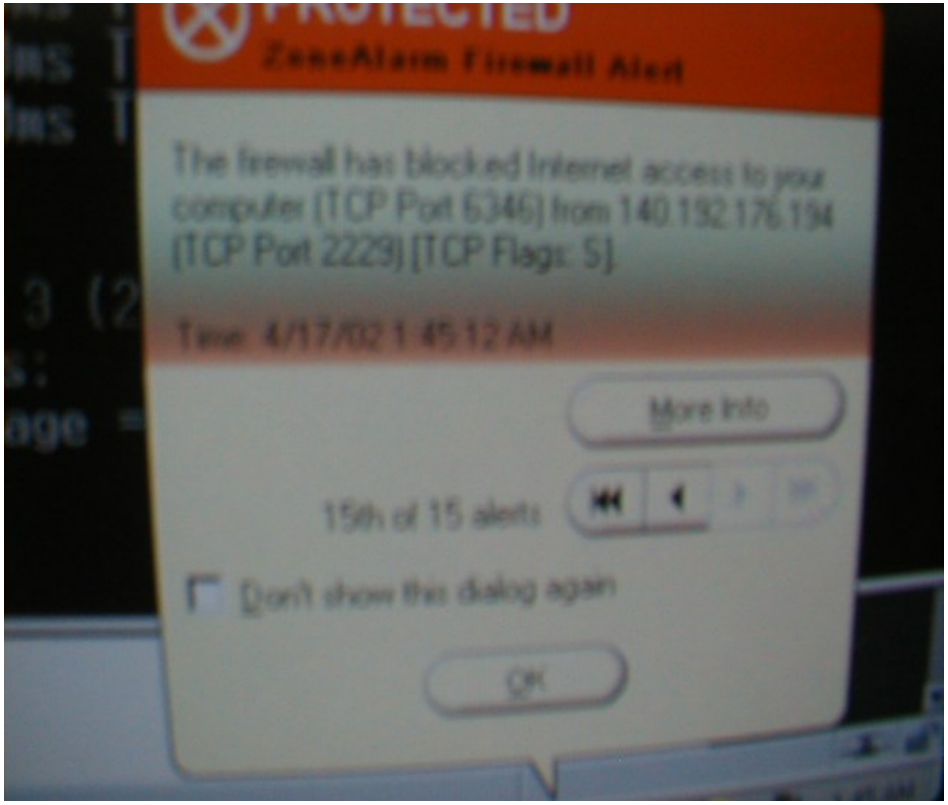
Aren't they just all kiddies?

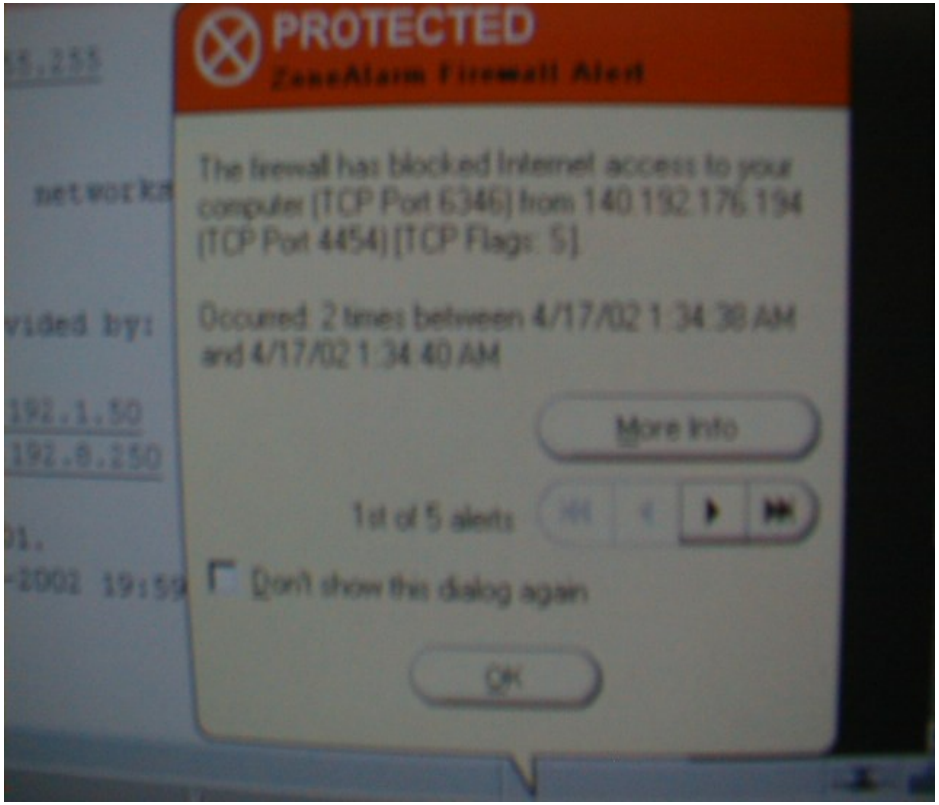
- There are a lot of kids, but no, it's not all kids
- And it's not all about the laughs, not anymore
- Internet crime is easy money with low risk
  - Miscreants, with much lower IQs than you and I, are out there h4x0ring it up making hundreds, maybe thousands of dollars a month while you're paying to sit here and listen to me babble. Doesn't that s**k?!
- Actually, some miscreants aren't so dumb, and look around, many of them look like any one of us

People, people just s**k!

- Yes, human nature is a ultimately a key contributor
  - Users do dumb things
  - Miscreants, they exist, that s*x
  - Vendors, programmers, operators can be dumb
  - Government and legal entities can be clueless
- On the bright side
  - There's lot of cool apps, games and multimedia
  - You can do serious research from your home
  - and... when given lemons...

Complaint


ZoneAlarm Firewall Alert
The firewall has blocked Internet access to your computer (TCP Port 6346) from 140.192.176.194 (TCP Port 2229) [TCP Flags: S]
Time: 4/17/02 1:45:12 AM
More Info
15th of 15 alerts
Don't show this dialog again
OK


PROTECTED
ZoneAlarm Firewall Alert
The firewall has blocked Internet access to your computer (TCP Port 6346) from 140.192.176.194 (TCP Port 4454) [TCP Flags: S]
Occured: 2 times between 4/17/02 1:34:38 AM and 4/17/02 1:34:40 AM
More Info
1st of 5 alerts
Don't show this dialog again
OK

Parting Shot

The end

- For future reference, you can find me her
  - http://www.cymru.com/jtk/
  - http://condor.depaul.edu/jkristof/