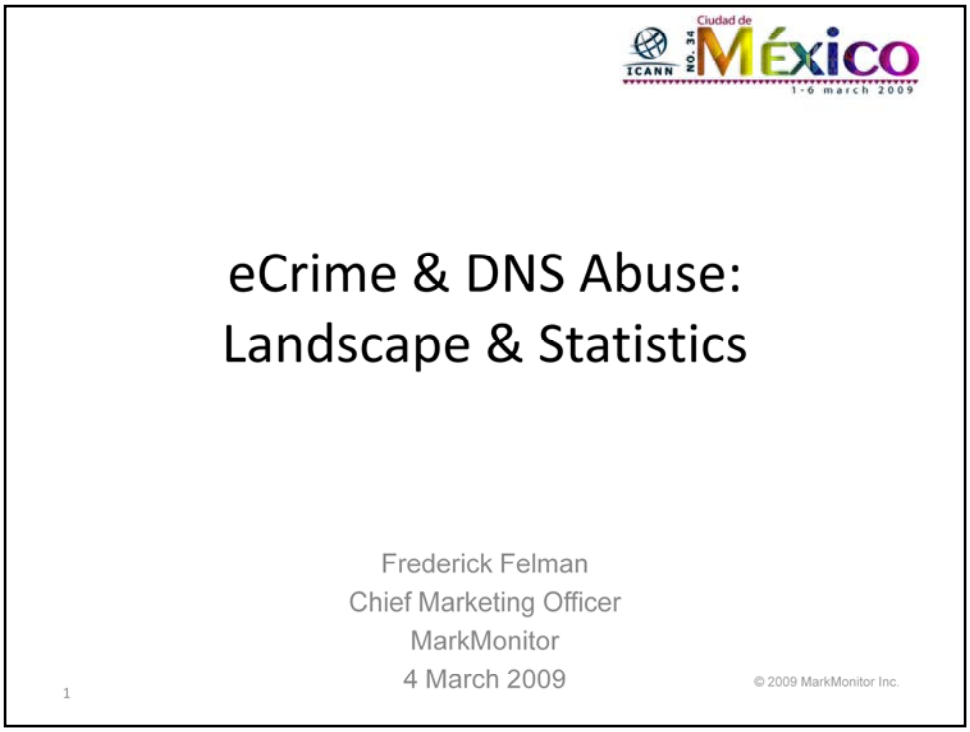
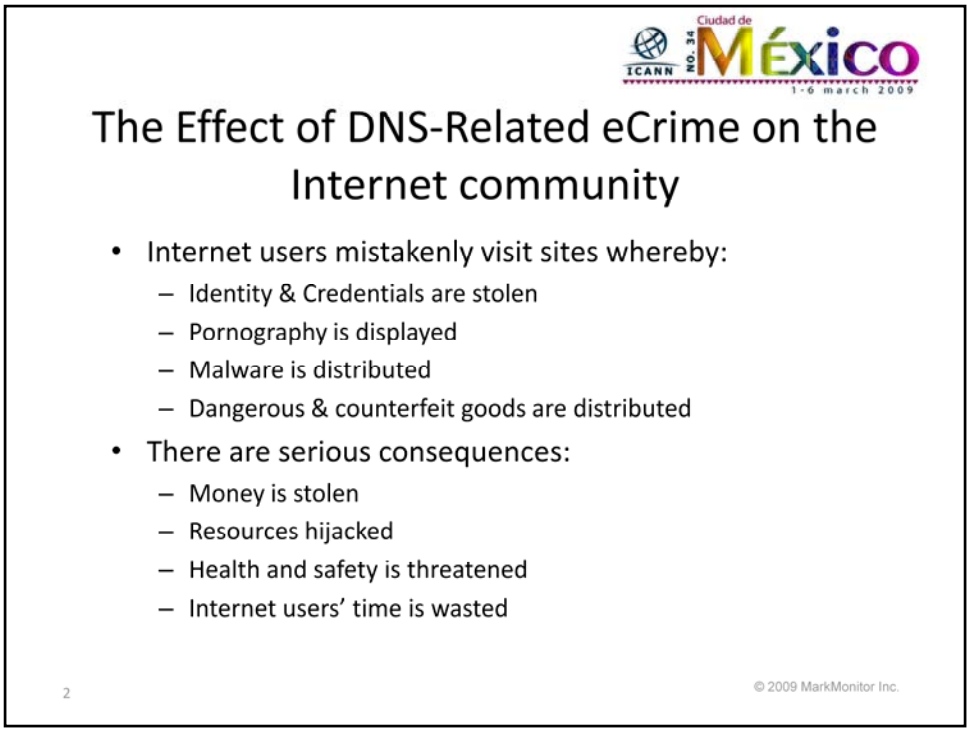


Trust and confidence in the online world, in the Internet, and in the DNS itself are key elements of importance to businesses and the over 1.6 billion Internet users that they serve through applications and services. Of course, none of these are ICANN's responsibility, but the underlying infrastructure of unique inidicators that ICANN coordinates is, in some cases, being exploited, or abused, and that is what you are going to talk about -- current real case examples and statistics.

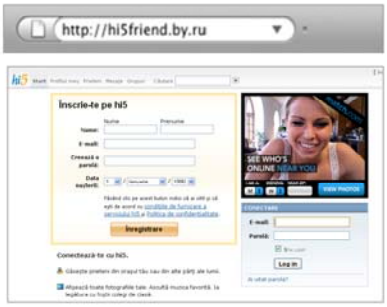


Isn't it more like: Internet users access sites other than those they intended to reach -- accidently, or through misdirection -- or access a site without understanding it has risks or presents illegal or undesirable content from their perspective.

Instead of confidentiality compromised -- isn't it privacy breached when private contact details, or Personally Identifiable details are collected inappropriately or illegally?

Are you going to say something like "trust and confidence in the DNS itself is part of trust and confidence in the broader Internet and WWW? or contributes to?

Cybersquatting & Credential Theft/Phishing



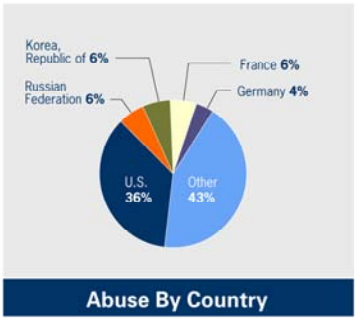
- 7.3% YOY (2007-2008) increase in number of companies phished
- Hundreds of thousands of attacks each year
- Large numbers exploiting fast-flux networks
- 51% increase in targeted attacks against Financial Institutions in latter part of 2008
- US$ 3.2B Total and US$ 886 per incident losses in 2007 (Gartner)
- 60-70% of attacks are domain-name based

3

135% increase vs “others” (11,000 attacks)

Though many hacked sites originate attacks or botnets direct the resolving site is an owned domain. Oftent insignificant name.

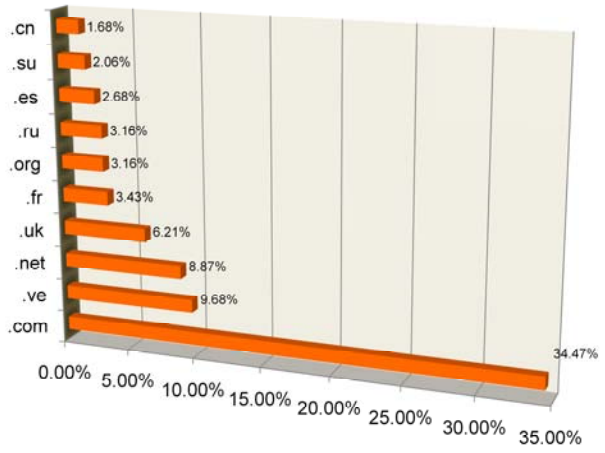
Phishing Host Country



Abuse By Country

- U.S. leads hosting countries with 36% of phishing sites in 2008
- Canada #7 over the year and new to the top 5 in Q4
- Top 5 by Quarter
  - Q1: United States; Russian Federation; Hong Kong; Rep. of Korea; Thailand
  - Q2: United States; China; Russian Federation; Rep. of Korea; Romania
  - Q3: United States; France; Rep. of Korea; Russian Federation; Germany
  - Q4: United States; Rep. of Korea; France; Canada; Russian Federation

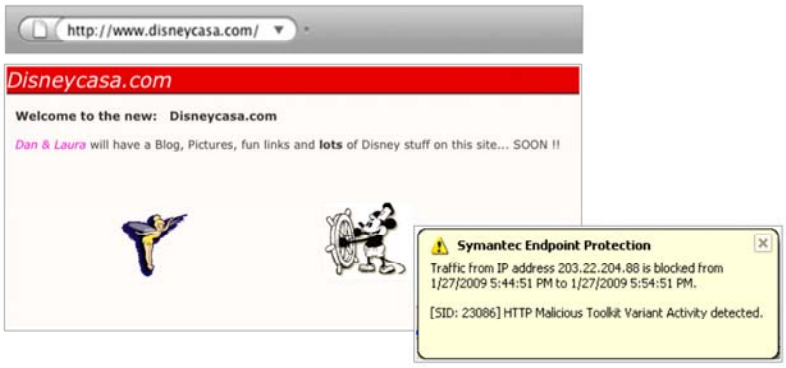
2008 Phishing TLD Host (%'s)
(as resolved in browser)



Cybersquatting & Display of Pornography

- 21% YOY (2007-2008) increase
- 1600 Sites targeting 30 companies

Cybersquatting & Malware Distribution



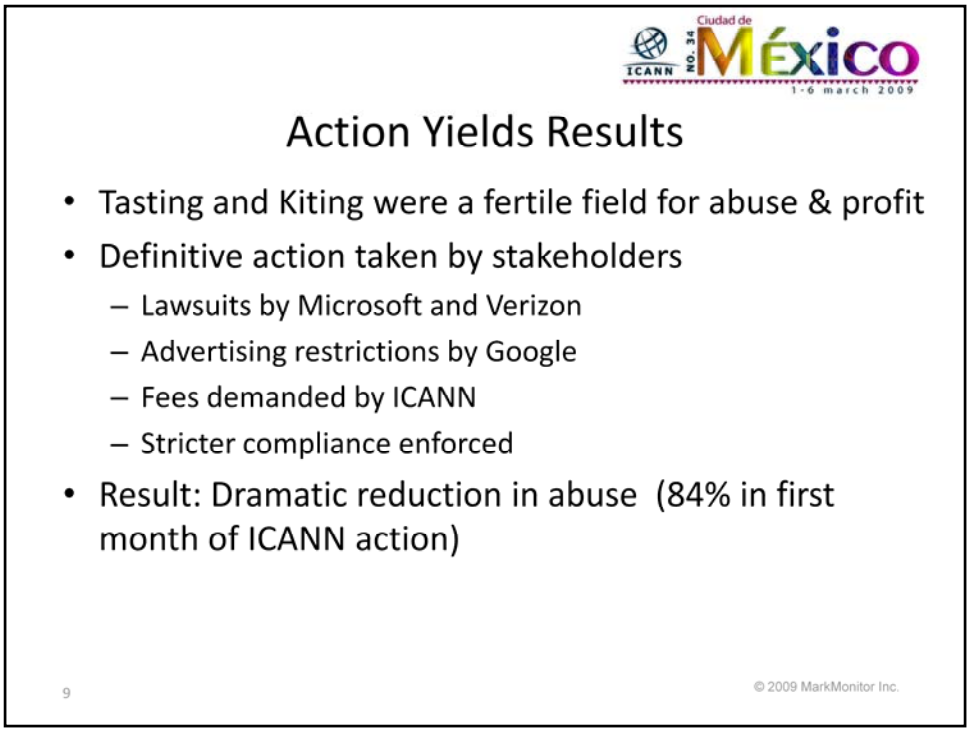
- More attacks in 1H 2008 than in all previous years combined*
- Over 1000 web-based attacks against social networks alone*

* McAfee 2009 Threat Predictions

Cybersquatting & Illicit Pharmaceuticals

- Nearly 3000 examples*
- Only 2 certified Pharmacies
- "Ongoing" businesses
- Many examples of "blended" threats (cybersquatting, illicit goods & malware)
- Pharmaceutical products drive 51% of spam according to Knujon

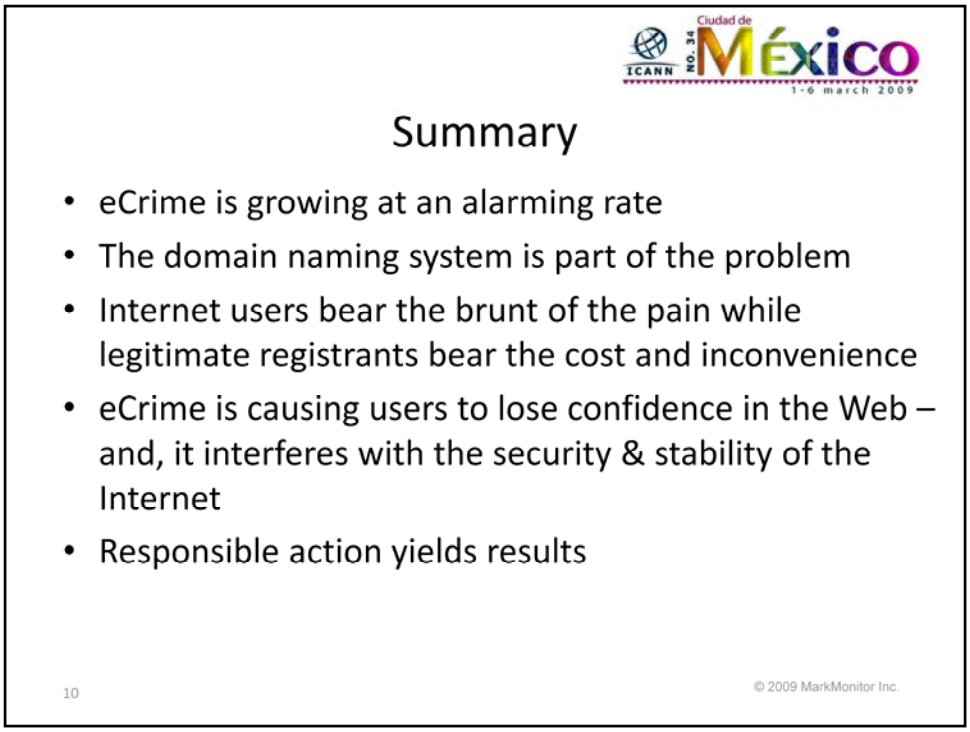
*Brandjacking Index™



All crime is growing at an alarming rate -- both offline and online
e-crime is now recognized as growing ..???
Users often put themselves at risk through lack of information, or through dealing with online misdirection, etc.

"brunt of the pain"might be better stated as Internet users and legitimate registrants of URLs bear the cost -- both in time, money, and in repercussions of there is loss of identity, or exploitation of resources?

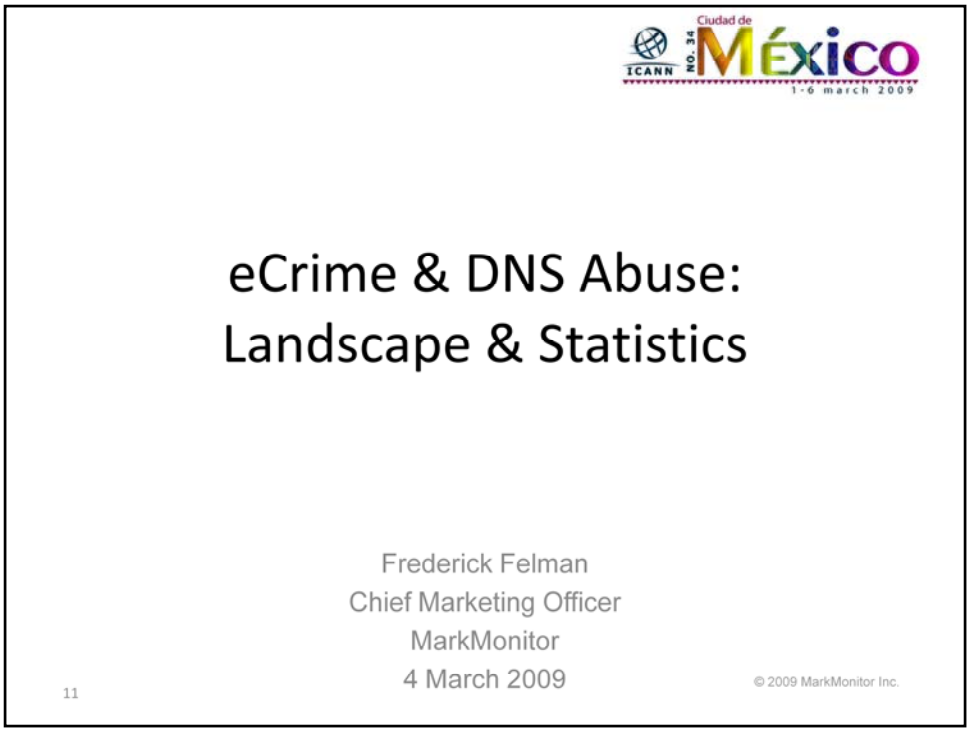
something like that..
I think you can both acknowledge that there is no single responsible entity, and that while it is a dangerous world, that safeguards and user awareness, and mechanisms to deal with risks can often limit harm.



All crime is growing at an alarming rate -- both offline and online
e-crime is now recognized as growing ..???
Users often put themselves at risk through lack of information, or through dealing with online misdirection, etc.

"brunt of the pain"might be better stated as Internet users and legitimate registrants of URLs bear the cost -- both in time, money, and in repercussions of there is loss of identity, or exploitation of resources?

something like that..
I think you can both acknowledge that there is no single responsible entity, and that while it is a dangerous world, that safeguards and user awareness, and mechanisms to deal with risks can often limit harm.



Trust and confidence in the online world, in the Internet, and in the DNS itself are key elements of importance to businesses and the over 1.6 billion Internet users that they serve through applications and services. Of course, none of these are ICANN's responsibility, but the underlying infrastructure of unique inidicators that ICANN coordinates is, in some cases, being exploited, or abused, and that is what you are going to talk about -- current real case examples and statistics.