MYNIC Berhad

Domain Hijacking &
Relationship with CERT (MYCERT)
- Policy/Legal perspective

ccNSO members meeting
5th November 2008

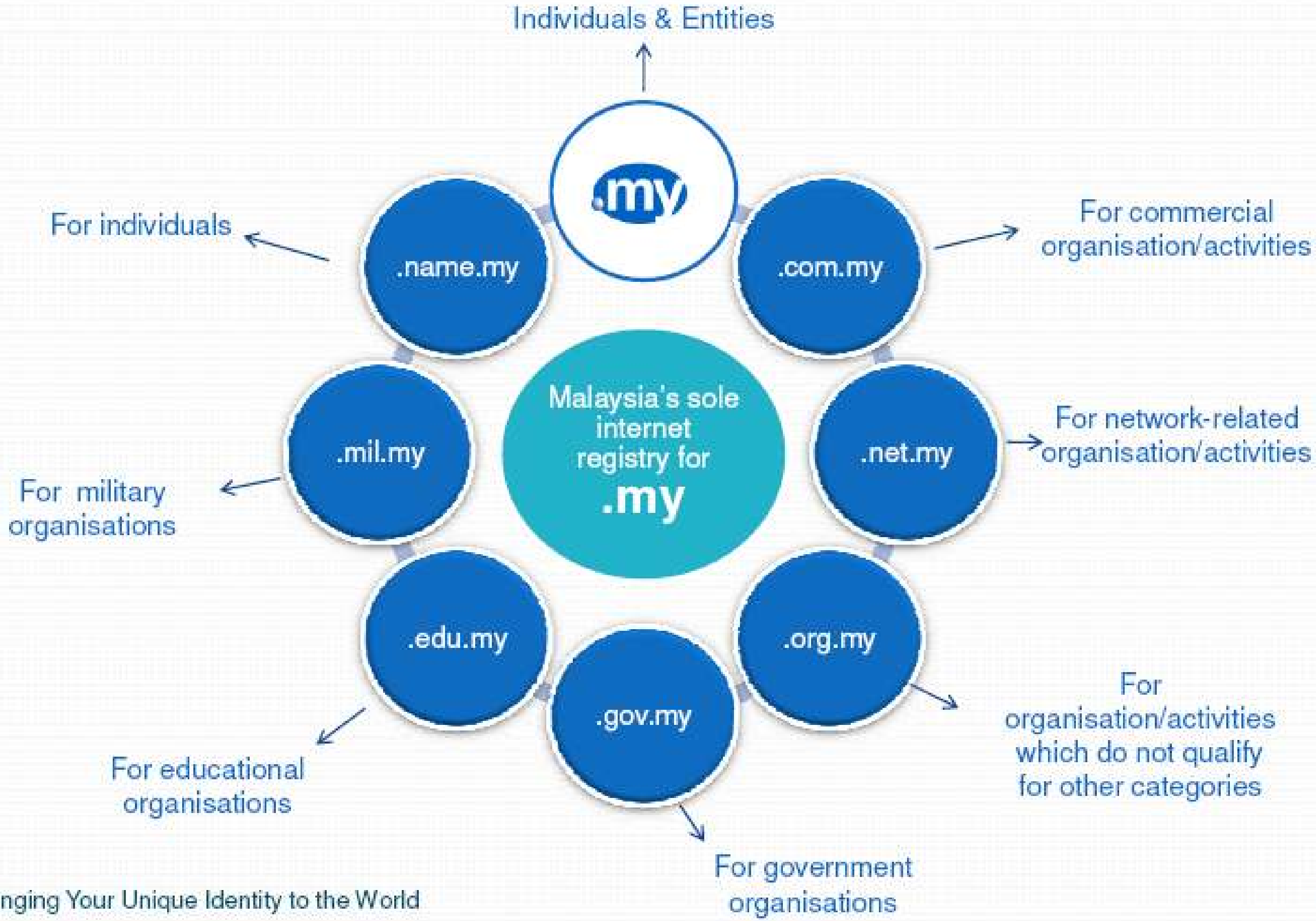
MYNIC Berhad
www.mynic.my

MYNIC - Overview

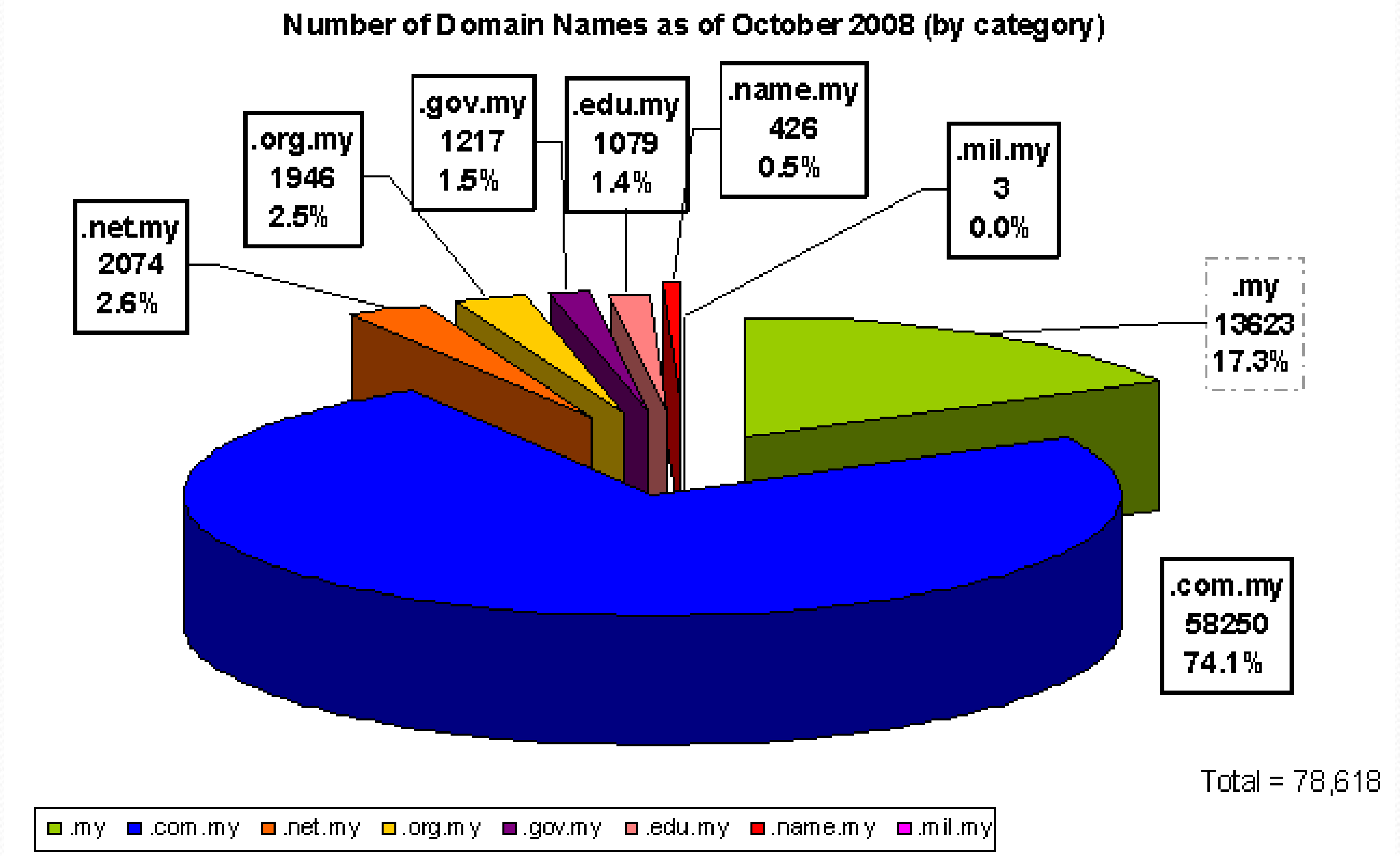
History

1987 - 2006	• Established as a division of MIMOS Berhad
December 2006	• Became a legal entity under the Ministry of Science, Technology & Innovation • Regulated by the Malaysian Communication and Multimedia Commission • Communications and Multimedia Act 1998 • Not for profit

Domain Name Registration


Individuals & Entities
.my
For individuals
.name.my
.com.my
For commercial organisation/activities
.mil.my
Malaysia's sole internet registry for .my
.net.my
For network-related organisation/activities
For military organisations
.edu.my
.org.my
.gov.my
For organisation/activities which do not qualify for other categories
For educational organisations
For government organisations

Statistics of ".my" category of domain names (Oct 2008)



Summary of Presentation

- Definition of Domain Hijacking
  - Domain Names
  - Domain Name System (DNS) resource records
  - APTLD Internet Security Survey 2008
- Lessons from UDRP
- SSAC report on “hushmail.com”
- MYNIC’s relationship with MYCERT
- Legal/Policy on domain hijacking
  - Malaysian Penal Code
  - Communications & Multimedia Act 1998
  - Legal Issues in CyberSpace

Domain Hijacking

Definition

Domain Hijacking

- Wrongful taking of control of a domain name from the rightful name holder.

  [Source: SSAC Report on Domain Name Hijacking: Incidents, Threats, Risks, & Remedial Actions, 12th July 2005]

Specific Issue

DNS Hijacking

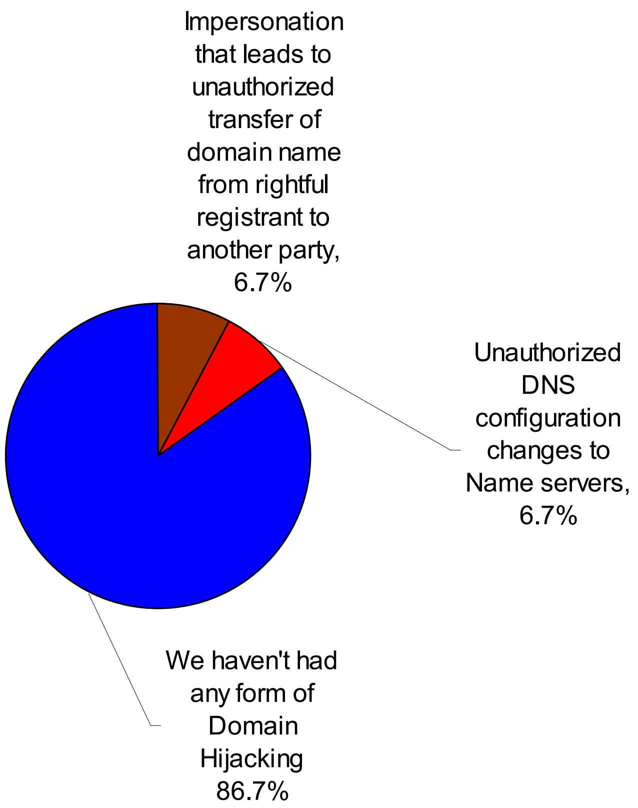
- Illegal change to DNS server that directs a URL to a different website. In some cases, the new website's URL may have one different letter in the name that might go unnoticed. The bogus website might offer similar and/or competing products for sale, or it may be a vehicle to publicly smear the reputation of the intended website. See **DNSSEC**, **DNS cache poisoning** & **pharming**.

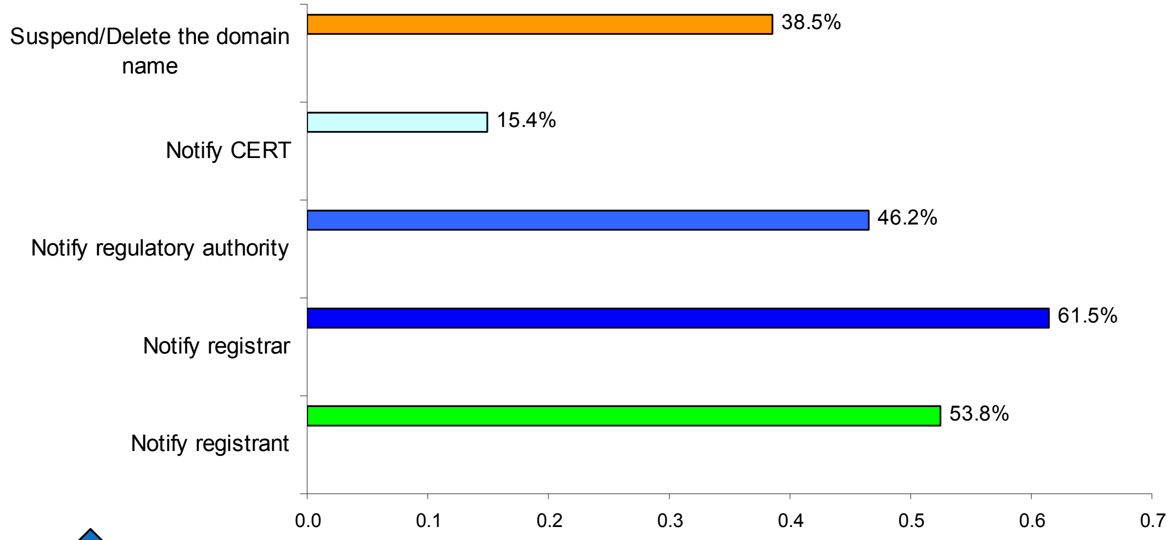
  [Source: Zul Rafique & Partners]

APTLD Internet Security Survey 2008

- April – June 2008
- 22 respondents from 19 ccTLDs

What forms of DN hijacking does your ccTLD registrants experience?





What action does your ccTLD take when a complaint is directed to you?

Lessons from UDRP

- Unauthorized transfer of domain name

“wei.com” (WIPO Case No. D2004-0955)

“The Complainant seeks to expand the territory of bad faith, presenting a new type of abusive conduct on the part of the Respondent, one that on its face cries out for relief: ***the hijacking of domain name through the manipulation of password access. Equitable considerations aside,*** *the Panel must determine whether the unusual facts of this matter bring the Complaint within the framework of the Policy”*

Facts which Panel found sufficient to estb. bad faith under para 4(a)(iii) of the Policy:

- Respondent knew or ought to have known domain name was in use and had been used for many years in connection with an active website;
- Respondent gained access to the Registrar ownership database through improper (likely fraudulent) means;
- Respondent changed the ownership records for the domain name covertly, without any notice to the rightful owner;
- Respondent used misleading & false contact information when it changed the ownership records;
- Respondent failed to respond to correspondence from Complainant, & never offered any explanation or justification for its conduct;
- Respondent disrupted the legitimate business activities of the Complainant, depriving it of access to the domain name & website it had created & maintained for more than 10 years

Lessons from UDRP

- Unauthorized transfer of domain name

“direction.com” (WIPO Case No. D2007-0605)

“It appears that Respondent had unlawfully hijacked the Domain Name through ***deception*** *and* ***thievery****.”*

Panel found there was bad faith registration and use on the following basis:-

- Respondent gained control of Domain Name
  - WITHOUT the permission of the Complainant and
  - through IMPROPER means

- Respondent appears to have changed the registration details for the D.N. covertly, without giving notice to Complainant or obtaining its authorization

- Respondent used an email address that has allegedly been linked to other instances of domain theft

Lessons from UDRP

- Unauthorized transfer of domain name

"jai.com" (WIPO Case No. D2007-1685)

Panel found there was bad faith registration and use on the following basis:-

- Respondent gained control of Domain Name
  - WITHOUT the permission of the Complainant and likely
  - through IMPROPER means

"It is well-settled that the practice of hijacking a domain name i.e. wrongfully taking control of a domain name from the rightful name holder (cf. ***Domain Name Hijacking: Incidents, Threats, Risks, and Remedial Action, Report from the ICANN Security and Stability Advisory Committee, July 12, 2005****), is of itself evidence of bad faith use and registration of a domain name"*

- Finding further supported by fact that Respondent previously found to have hijacked and thus registered and used in bad faith two other domain names by NAF panels

Olympic Credit Fund, Inc. v. Site Services International c/o Richard Sorensen, NAF Case No. FA 910790 ("ocf.com");

Wall Street Webcasting & Douglas Estadt v. Site Services International c/o Richard Sorensen, NAF Case no. FA 955052 ("wsw.com")

SSAC report on “hushmail.com”

- Unauthorized DNS configuration changes to name servers

- Attacker convinced Registrar to modify AC’s email contact info. in Hush’s registration record

- Attacker used AC email address to submit password reset request

- Attacker accessed Hush Communications account, changed password & used account to alter DNS configuration; attacker pointed the domain name A record to attacker’s server

- Attacker posted a defaced home page expressly designed to embarrass Hush Communications & gain notoriety for attacker

Difference:-

No transfer of domain name

- CTO of Hush Communications used BC to access Hush’s account, reset password, restored AC information & correct DNS configuration

- ISP that hosted hoax page shut it down: chronology of events leading to this still under investigation by Royal Canadian Mounted Police

- Happened same time that Registrar was contending with denial of service (DOS) attacks directed against its name servers

Conclusion: SSAC’s 10 recommendations on remedial actions

SSAC report recommendations

- Ten (10) but am focusing on Registries & ICANN role
- Registries should

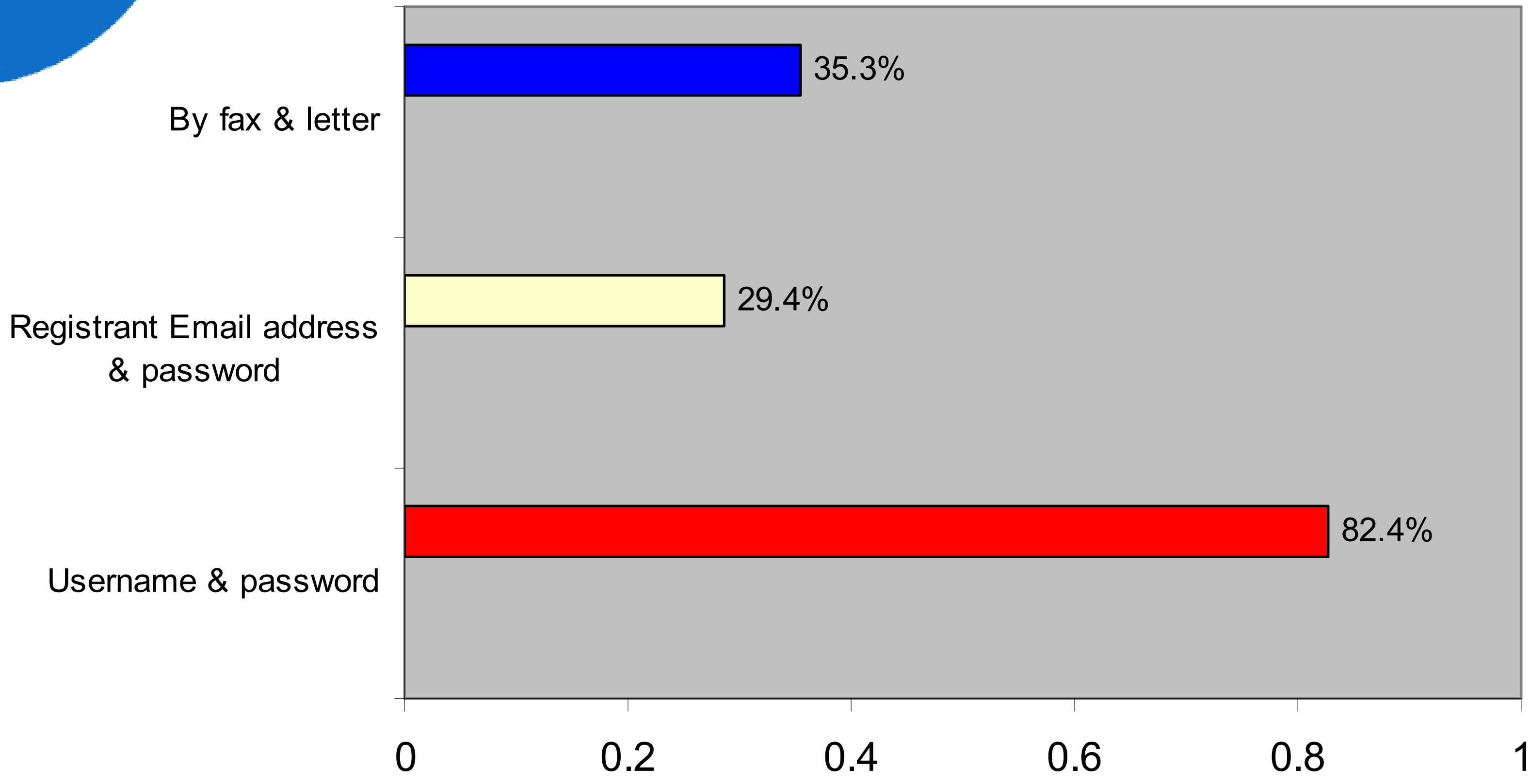
1) Ensure Registrar-Lock & EPP authInfo are implemented according to specification;
2) (& Registrars) Provide resellers & registrants with best Common Practices that describe use & assignment of EPP authInfo codes & risks of misuse;
3) (ICANN & Registrars) Public awareness campaign to identify criteria & procedures for registrants to follow to request immediate intervention & obtain immediate restoration of d.n. & DNS configuration;

- ICANN should

4) Investigate whether stronger & more publicly visible enforcement mechanisms are needed to deal with registrars that fail to comply with the transfer policy, & hold registrars accountable for actions of their Resellers;
5) Consider whether to strengthen the identity verification requirements in electronic correspondence to be commensurate with the verification used when the correspondence is by mail or in person

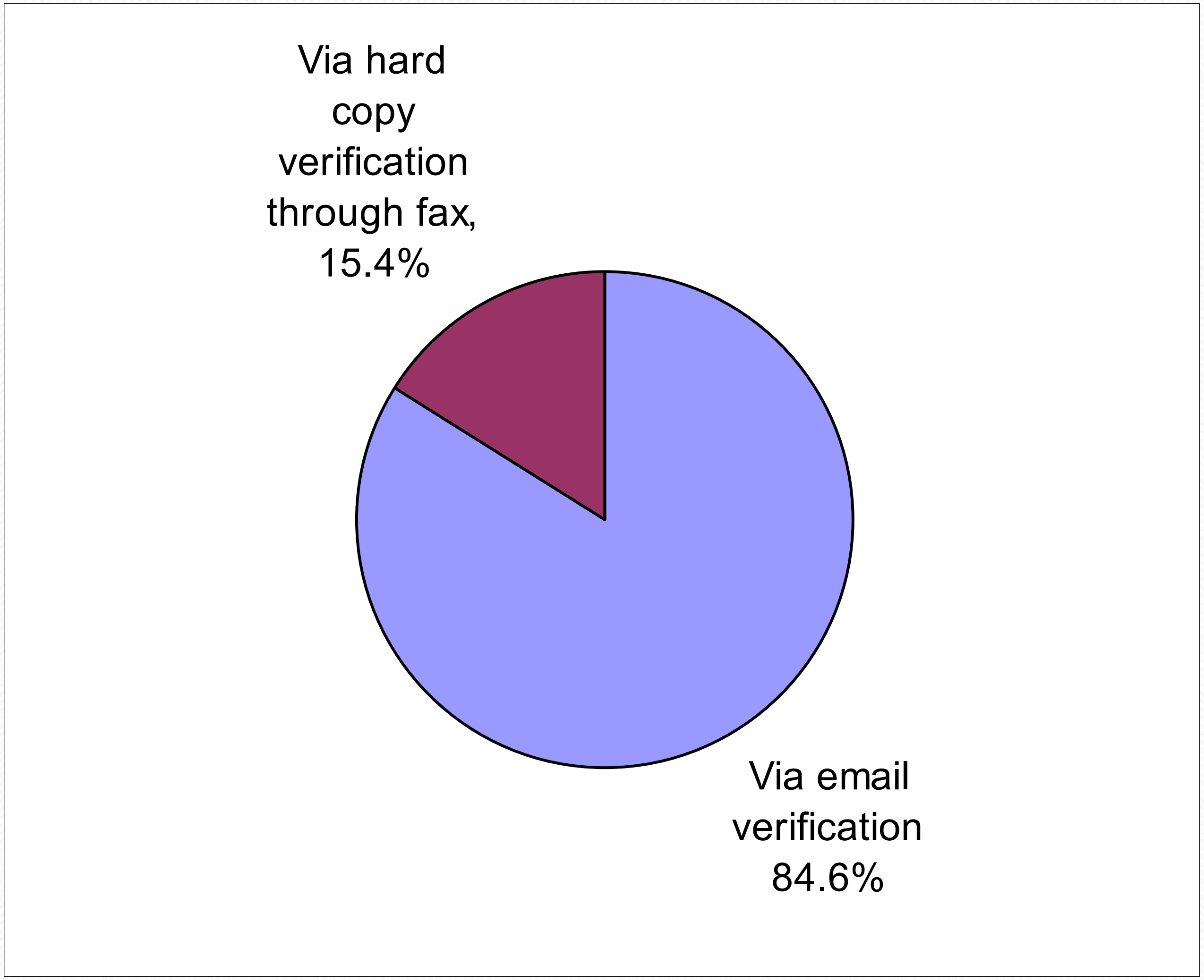
APTLD Internet Security Survey 2008

What are the security measures your ccTLD provide to allow changes to Registrants' contact information?



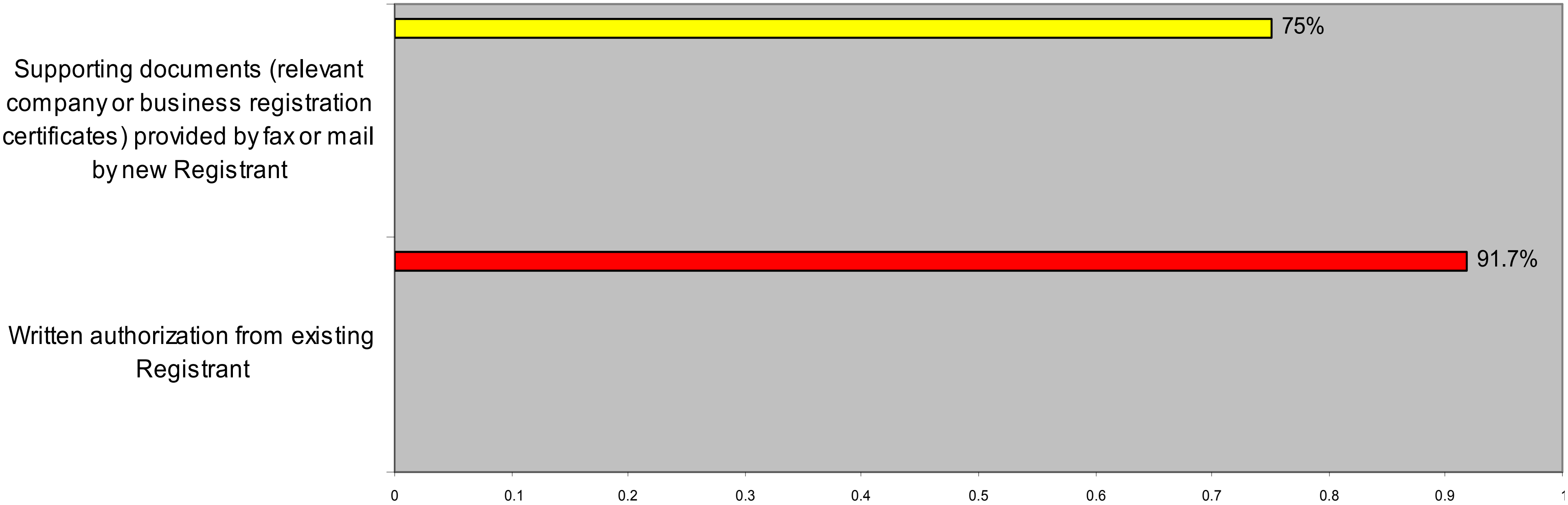
APTLD Internet Security Survey 2008

How are the security measures (e.g. username & password) provided to your Registrants?



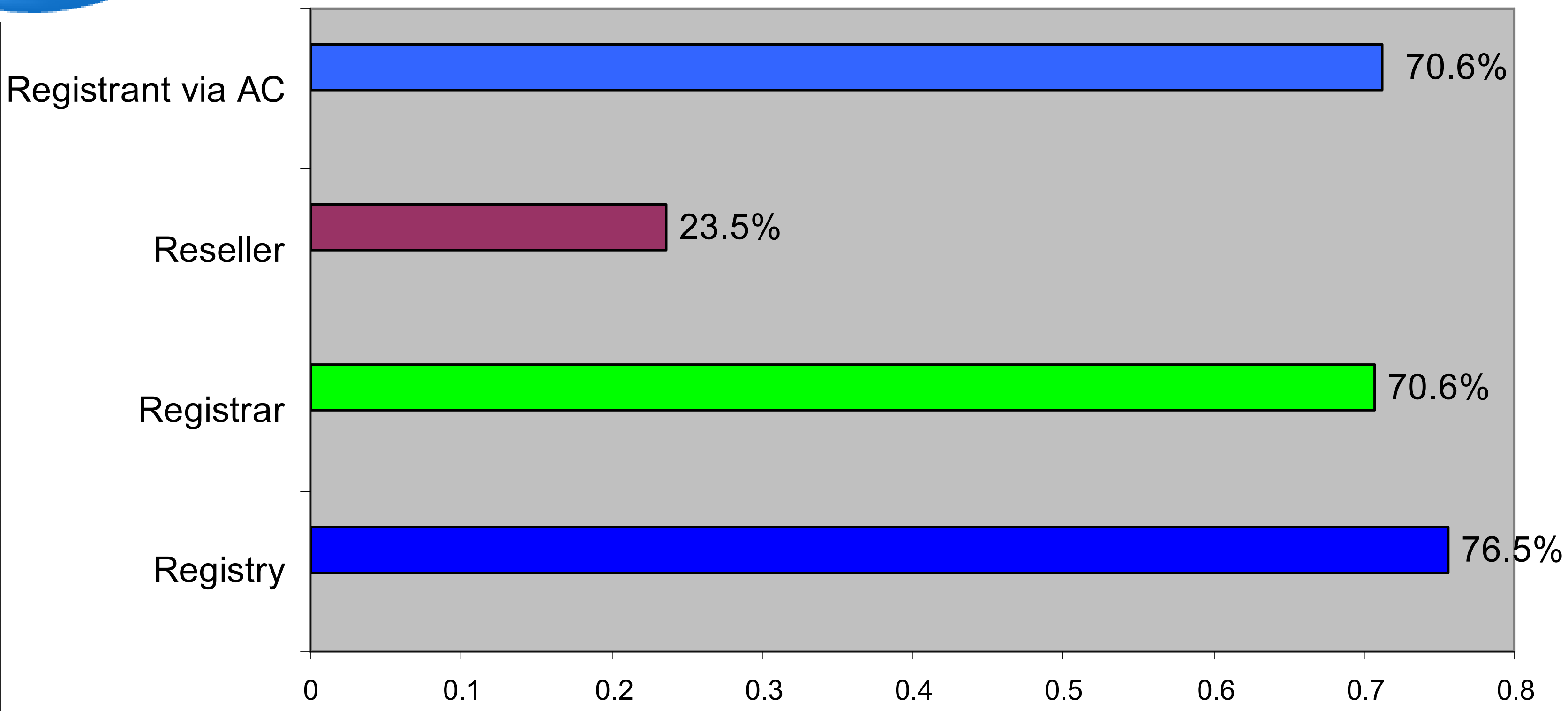
APTLD Internet Security Survey 2008

What are required to transfer the domain name from existing Registrant to new Registrant?



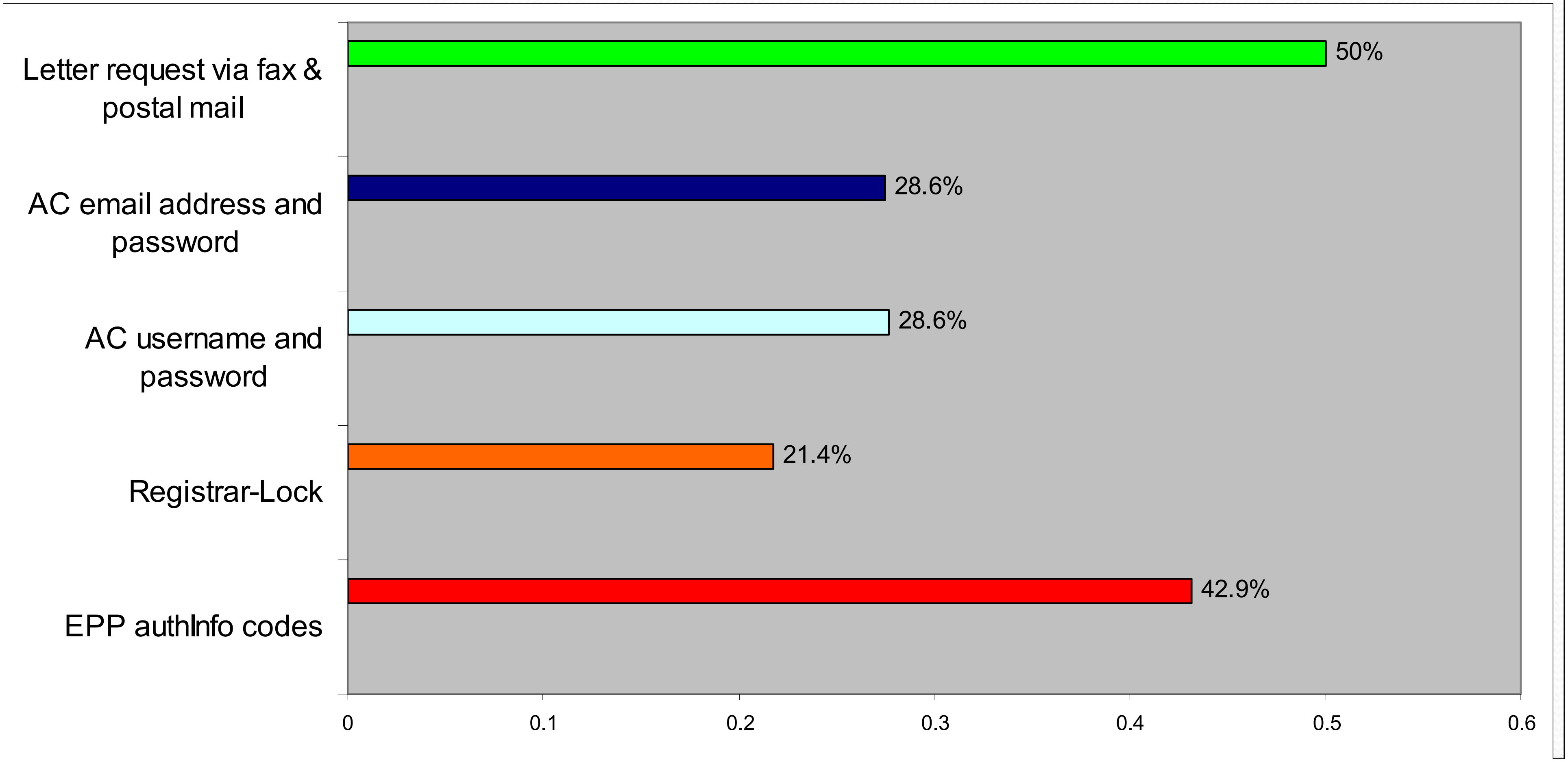
APTLD Internet Security Survey 2008

Who is/are involved in the transfer of domain name from existing Registrant to new Registrant?



APTLD Internet Security Survey 2008

What security measures are involved in the transfer process?



Relationship with CERT – Malaysian Computer Emergency Response Team (MYCERT)

MYNIC & MYCERT relationship

- Complementary

  - Tips to safeguard yourself from fraudulent email/phishing attempts

http://www.mycert.org.my for CYBER999 REPORTING INCIDENTS & ALERTS MyCERT Malaysian Computer Emergency Response Team

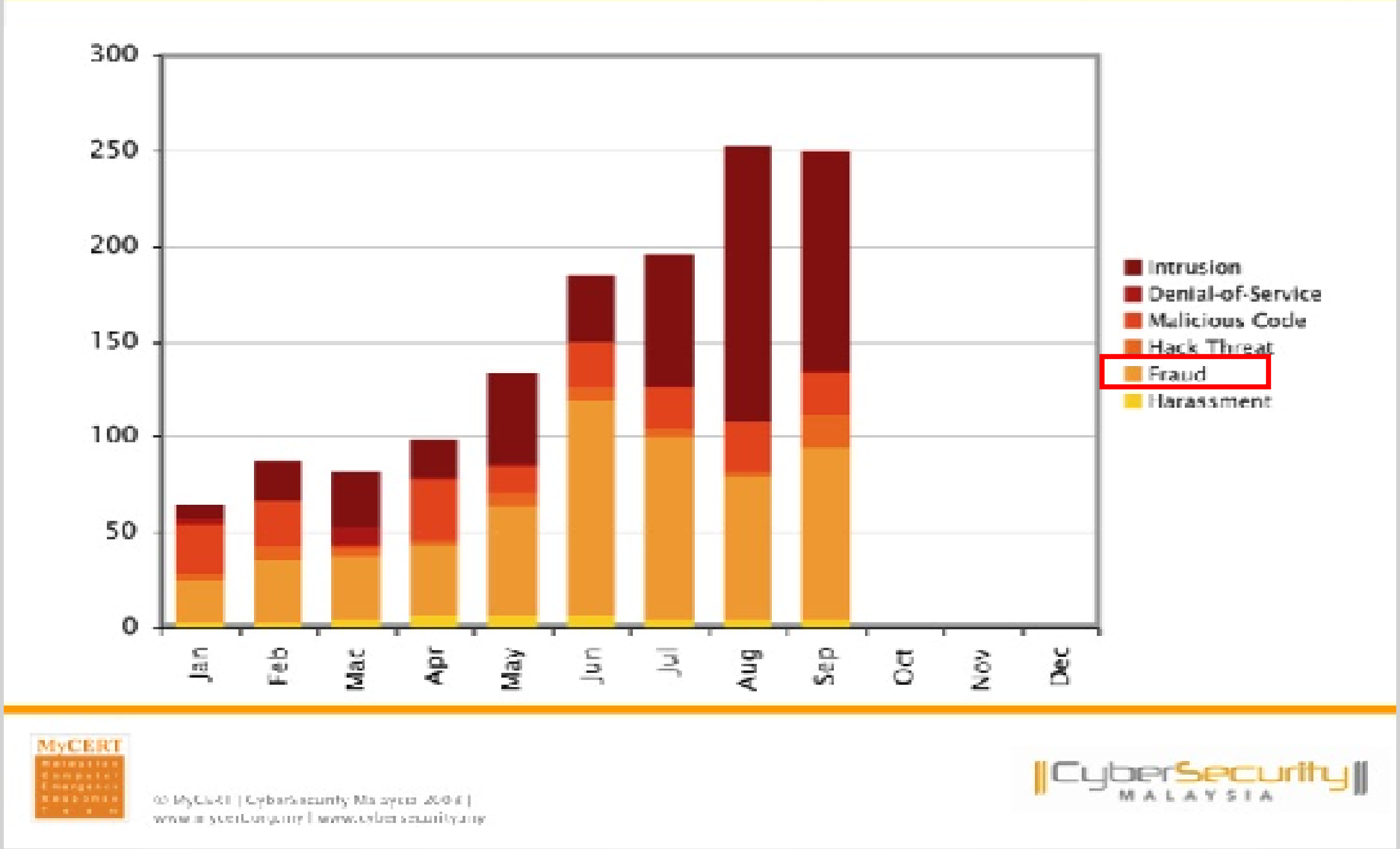
Technical website

cyber999@cybersecurity.org.my → for incidence reporting

- WHOIS public tool for MYCERT to alert TC of compromised “my” domain names or locate IP address where the phishing site is hosted

[http://whois.mynic.my]

Incident Statistics for 2008



	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	TOTAL
Harassment	2	2	4	6	6	6	4	4	4	-	-	-	38
Fraud	22	33	33	37	57	112	95	75	90	-	-	-	554
Hack Threat	4	7	4	2	7	7	5	2	17	-	-	-	55
Malicious Code	26	24	29	32	14	25	21	26	22	-	-	-	219
Denial of Service	3	0	2	1	1	0	1	0	1	-	-	-	9
Intrusion	7	21	9	20	48	35	70	145	116	-	-	-	471
TOTAL	64	87	81	98	133	185	196	252	250	-	-	-	-

Internet Banking Task Force (IBTF)

- Set up in 2004
- Industry-based estb. by Central Bank of Malaysia
- Develop industry-wide best practices & collaborate with relevant agencies to handle security infringement incidences
- Special emphasis on thwarting phishing & other forms of identity theft frauds
- 19 commercial banks in Malaysia are members of IBTF (banks providing Internet banking services in Malaysia)
- IBTF members include MCMC, CyberSecurity & Royal Malaysian Police.
- Meeting in April 2008 to discuss “Incident Response Plan” involving MYCERT & IBTF members

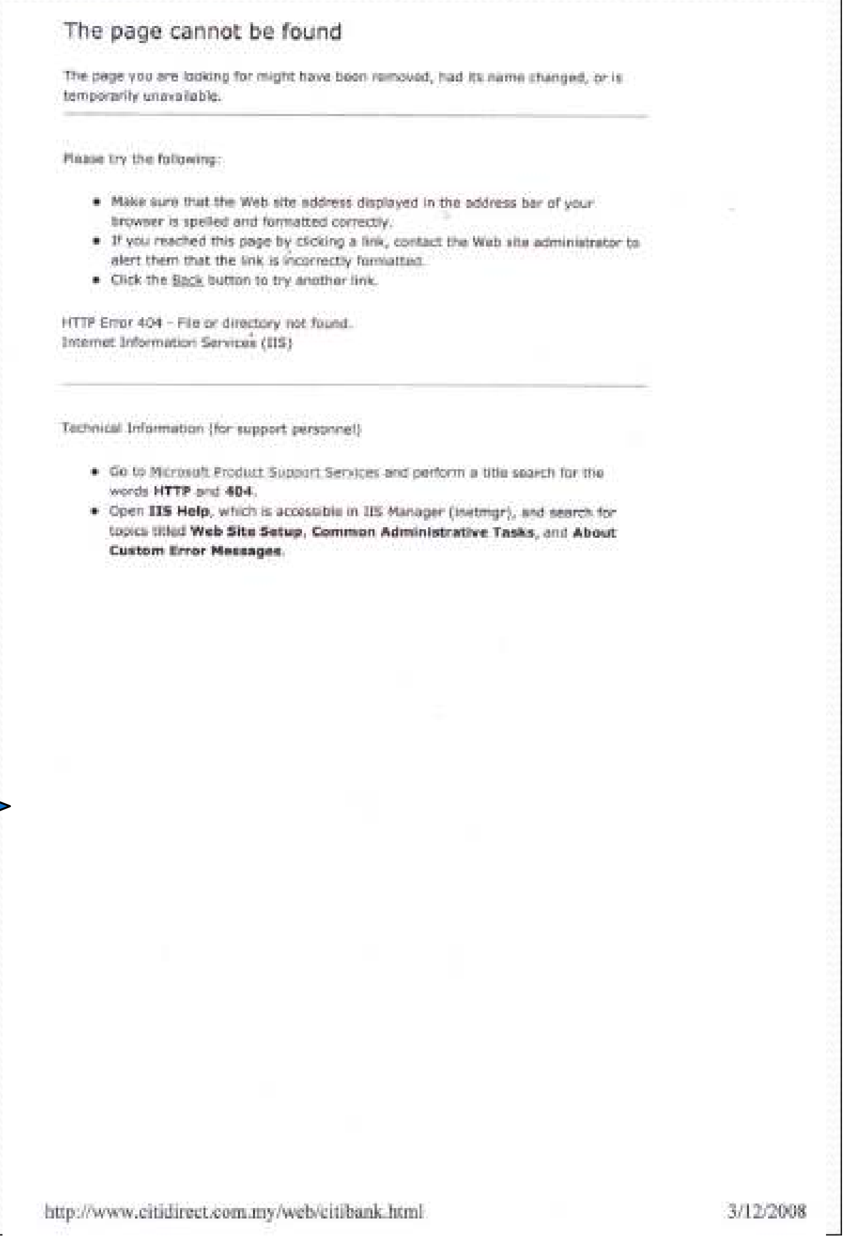
(Platform for sharing information)

[“Payment & Settlement Systems”, Bank Negara Malaysia at Page 222]

www.citidirect.com.my/web/citibank.html

- Domain name registrant

  www.citidirect.com.my
- Complaint by renown financial institution to MYNIC & MYCERT on 28th March 2007
- MYNIC liaised with MYCERT & MCMC
- MYCERT responded to foreign bank's anti-phishing group on 29th March 2007
- Result
- MYCERT will continue to monitor incident



The page cannot be found

The page you are looking for might have been removed, had its name changed, or is temporarily unavailable.

Please try the following:

- Make sure that the Web site address displayed in the address bar of your browser is spelled and formatted correctly.
- If you reached this page by clicking a link, contact the Web site administrator to alert them that the link is incorrectly formatted.
- Click the Back button to try another link.

HTTP Error 404 - File or directory not found.
Internet Information Services (IIS)

Technical Information (for support personnel)

- Go to Microsoft Product Support Services and perform a title search for the words **HTTP** and **404**.
- Open **IIS Help**, which is accessible in IIS Manager (inetmgr), and search for topics titled **Web Site Setup**, **Common Administrative Tasks**, and **About Custom Error Messages**.

http://www.citidirect.com.my/web/citibank.html 3/12/2008

Policy/Legal considerations

Domain hijacking

Statutory Law – Penal Code of Malaysia on Cheating

- S. 415 – Offence of Cheating

  Whoever by deceiving any person, whether or not such deception was the sole or main inducement, intentionally induces the person so deceived to do … anything which he would not do … if he were not so deceived and which act … causes or likely to cause damage or harm to any person in body, mind, reputation, or property, is said to "cheat"

  Penalty:- Imprisonment (max: 5 years) or fine or both [s. 417]

- S. 416 – Offence of Cheat by Personation

  Cheats by pretending to be some other person or representing that he is a person other than he really is.

  Illustration:- by pretending to be a certain rich banker of the same name

  Penalty:- Imprisonment (max: 7 years) or fine or both [s. 419]

Malaysian Communications & Multimedia Commission (MCMC)

- **S. 263 Communications & Multimedia Act 1998**

(1) A licensee shall use his best endeavour to prevent the network facilities that he owns or provides or the network service, applications service or content applications service that he provides from being used in, or in relation to, **the commission of any offence under any law of Malaysia.**

(2) A licensee shall, upon written request by the Commission or any other authority, assist the Commission or other authority as far as reasonably necessary in **preventing the commission or attempted commission of an offence under any written law of Malaysia** or otherwise in **enforcing the laws of Malaysia**, including, but not limited to, the **protection of the public revenue** and preservation of national security.

General Legal DNS Issues in CyberSpace

- General Issue

  - Challenge in providing statutory definition of cybercrime

- Specific Issue

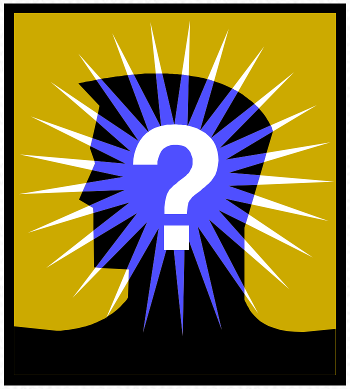
  - Cyber Fraud

    - Difficulty in proving the element on “intention”
    - Whether “intention” can be inferred from the e-mail that is made
    - Unauthorized transfer of domain name can amount to bad faith registration and use of domain names under UDRP
    - Unauthorized DNS configuration changes name servers
    - Phishing

- Specific Issue

  - Cyber Squatting

    - US Anti-Cybersquatting Consumer Protection Act 1999
    - MYDRP (16 cases filed as at October 2008)



Your Thoughts?

Email:- yeo@mynic.net.my

Senior Policy Executive, MYNIC Berhad

Domain Hijacking

Relationship with CERT

Policy

Law