# 2012 Google Pakistani Website Hack

(among others)

# …except that Google's website *wasn't hacked*

- On November 23rd, 2012, several notable websites were "defaced". A picture of two penguins and some Turkish writing being the only thing to appear when users tried to access those websites
- A group called Eboz was found to be involved, and likely responsible for matter. Eboz has been found to have a history of defacing websites, but not many as notable as the ones on that day.
- The list of websites that were affected can be found here
- Some notable examples include ebay.pk, microsoft.pk, yahoo.pk, and google.com.pk

eboz

Kankalarım hep yarımda arkadaş içinde
Yarımda olmayan mı var çekimlik her nefeste

?

trabzon 2012

Dostlara selam ölmedik hala yaşıyoruz!

# So what happened?

- How did a person/group manage to strike all these websites at the same time?
- Trick question. They didn’t.
- Instead of hacking, there was hijacking.

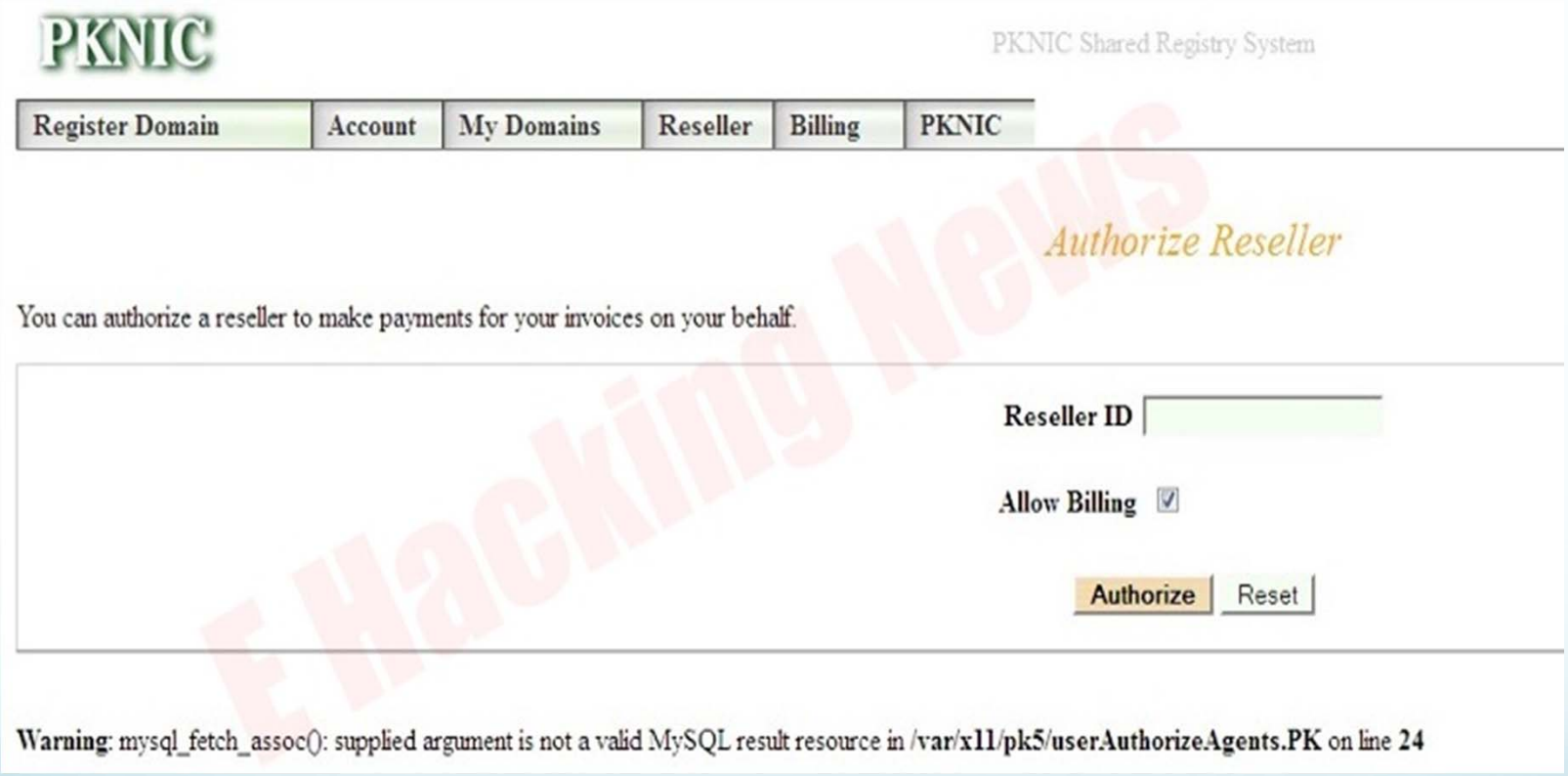
# PKNIC

- PKNIC is the domain name registry responsible for .pk
- Because of a vulnerability during a security upgrade, a Boolean-based SQL injection, the attacker to gain access to four PKNIC user accounts, which in turn compromised about nine DNS records.

# Boolean-based SQLi

- Formal definition: “Multiple valid statements that evaluate to true and false are supplied in the affected parameter in the HTTP request. By comparing the response page between both conditions, the tool can infer whether or not the injection was successful.”
- They did the SQL injections from PKNIC’s website

- They would do the SQLi on the PKNIC website and receive the following the screen, until they managed to access the accounts:



# A quick lookup

## DNS records

| name | class | type | data | time to live |
|---|---|---|---|---|
| google.com.pk | IN | A | 127.0.0.1 | 3600s(01:00:00) |
| google.com.pk | IN | NS | dns2.freehostia.com | 3600s(01:00:00) |
| google.com.pk | IN | SOA | server: dns1.freehostia.com | 3600s(01:00:00) |
| | | | email: support@freehostia.com | |
| | | | serial: 1353750918 | |
| | | | refresh: 28800 | |
| | | | retry: 7200 | |
| | | | expire: 604800 | |
| | | | minimum ttl: 86400 | |
| google.com.pk | IN | NS | dns1.freehostia.com | 3600s(01:00:00) |
| google.com.pk | IN | MX | preference: 10 | 3600s(01:00:00) |
| | | | exchange: mbox.freehostia.com | |

# It was DNS hijacking

- Many news media simply spread it around that the websites had been hacked, when in fact, users would simply be redirected to “dns1.freehostia.com” or “dns2.freehostia.com”, where the page in question was located.
- No credit card information or private information is stored on the affected servers but this still left many wary, believing still that Google and other sites were hacked.
- By simply modifying the records to how they were before, everything went back to normal.

# The End?

- Fast forward three months:

- This time it was by a group going by PAKbugs
- One of the reasons is because while everyone’s user accounts at PKNIC may have been reset following the Eboz attack, people likely changed their settings back to what it was before.

# Sources


- http://propakistani.pk/2012/11/26/pakistani-hackers-expose-pknic-vulnerabilities-defacements-of-pk-domains
- http://www.rafayhackingarticles.net/2012/11/how-google-pakistan-was-hacked.html
- http://www.ehtisham.com/2012/11/24/google-com-pk-hacked-technical-details-dns/
- http://techcrunch.com/2012/11/24/hacking-for-the-sake-of-it-eboz-downed-google-apple-300-other-pakistani-sites-and-many-more-just-to-show-it-can/
- https://www.us-cert.gov/sites/default/files/publications/Practical-SQLi-Identification.pdf