January 12 Baidu's Attack
- What Happened and What Shall We Do

WANG Zheng

中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

Background

ñBaidu.comò

- China's largest search engine.
- Claims 70 percent of China's Internet search market.
- Had only been down only once previously (for half an hour in December 2006).
- DNS records are managed by a New York - based company, Register.com.
- ...

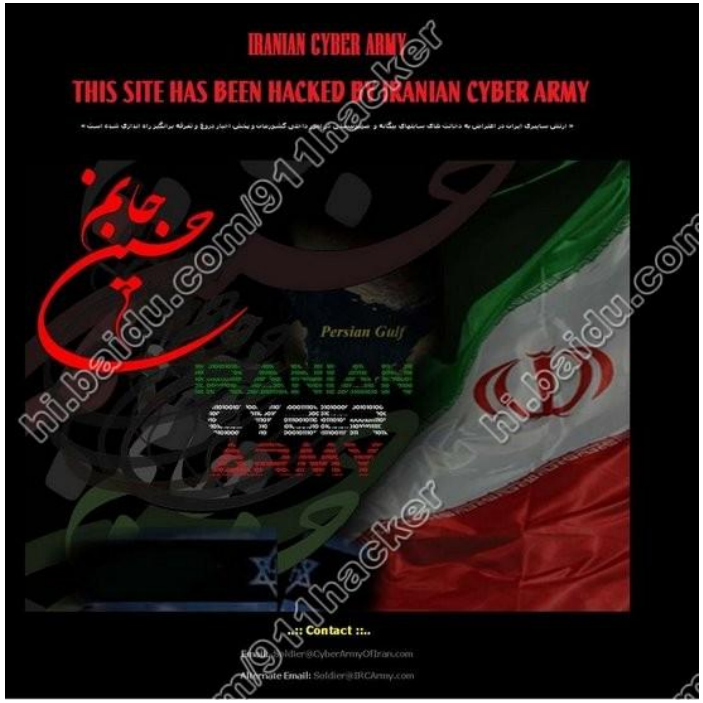
What happened – at first sight

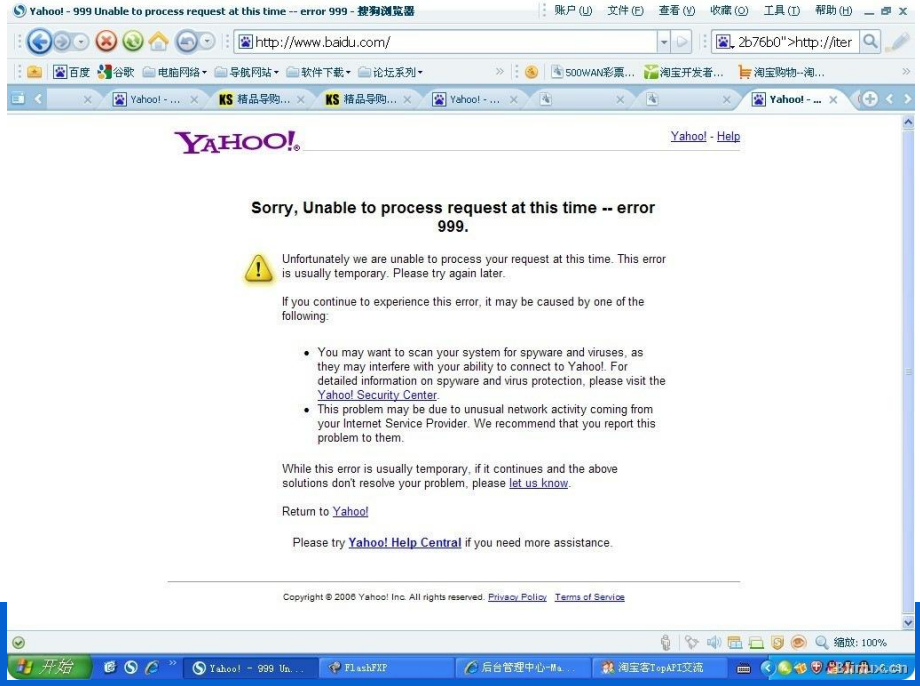
Baidu's home page hacked

- At about 7:40 am January 12th, Baidu went offline and at times a result of Baidu.com being redirected to a website located in the Netherlands.
- A screenshot of the defaced site showed an announcement in English that read: "This site has been hacked by Iranian Cyber Army".
- Some users tried to log onto Baidu.com, only to find it was inaccessible. Many others were redirected to a web error page of Yahoo!
- The site restored services for most Internet users by 6 pm.

中国互联网络信息中心
CHINA INTERNET NETWORK INFORMATION CENTER

Screenshots





What happened – some insights

How to ?

- Hackers ambushed the website by modifying the DNS records for the Baidu.com domain, redirecting visitors to another server.
- Hackers are believed to have broken through Baidu's account at Register.com and gained access to alter Baidu's DNS records.
- The redirected server was then flooded by the DNS requests, thus failed to respond.

Digged DNS information

Get DNS information in the breakdown using dig

◆9:01 Beijing Time: Request verisign's server

baidu.com.	172800	IN	NS	yns1.yahoo.com.
baidu.com.	172800	IN	NS	yns2.yahoo.com.

Yahooŝs server? Requests refused for Baidu.com.

Digged DNS information(cont'd)

◆9:36 Beijing Time: Request verisign's server

baidu.com.	172800	IN	NS	ns2303.hostgator.com.
baidu.com.	172800	IN	NS	ns2304.hostgator.com.

Requests success for Baidu.com, but the answers were not the IP addresses of baidu's web servers.

NS records were changed in the later request.

baidu.com.	172800	IN	NS	dns010.d.register.com.
baidu.com.	172800	IN	NS	dns050.c.register.com.
baidu.com.	172800	IN	NS	dns190.b.register.com.
baidu.com.	172800	IN	NS	dns204.a.register.com.

Whois information

Request Whois server for Baidu's information

◆9:02 Beijing Time:

Domain Name: BAIDU.COM
Registrar: REGISTER.COM, INC.
Whois Server: whois.register.com
Referral URL: http://www.register.com
Name Server: YNS1.YAHOO.COM
Name Server: YNS2.YAHOO.COM
Status: clientTransferProhibited
Updated Date: 11-jan-2010
Creation Date: 11-oct-1999
Expiration Date: 11-oct-2014

Whois information

◆9:50 Beijing Time:

Domain Name: BAIDU.COM
Registrar: REGISTER.COM, INC.
Whois Server: whois.register.com
Referral URL: http://www.register.com
Name Server: NS2303.HOSTGATOR.COM
Name Server: NS2304.HOSTGATOR.COM
Status: clientTransferProhibited
Updated Date: 11-jan-2010
Creation Date: 11-oct-1999
Expiration Date: 11-oct-2014

Whois information

◆10:51 Beijing Time:

Domain Name: BAIDU.COM
Registrar: REGISTER.COM, INC.
Whois Server: whois.register.com
Referral URL: http://www.register.com
Name Server: DNS010.D.REGISTER.COM
Name Server: DNS050.C.REGISTER.COM
Name Server: DNS190.B.REGISTER.COM
Name Server: DNS204.A.REGISTER.COM
Status: clientTransferProhibited
Updated Date: 11-jan-2010
Creation Date: 11-oct-1999
Expiration Date: 11-oct-2014

How to recover

The registrar side:

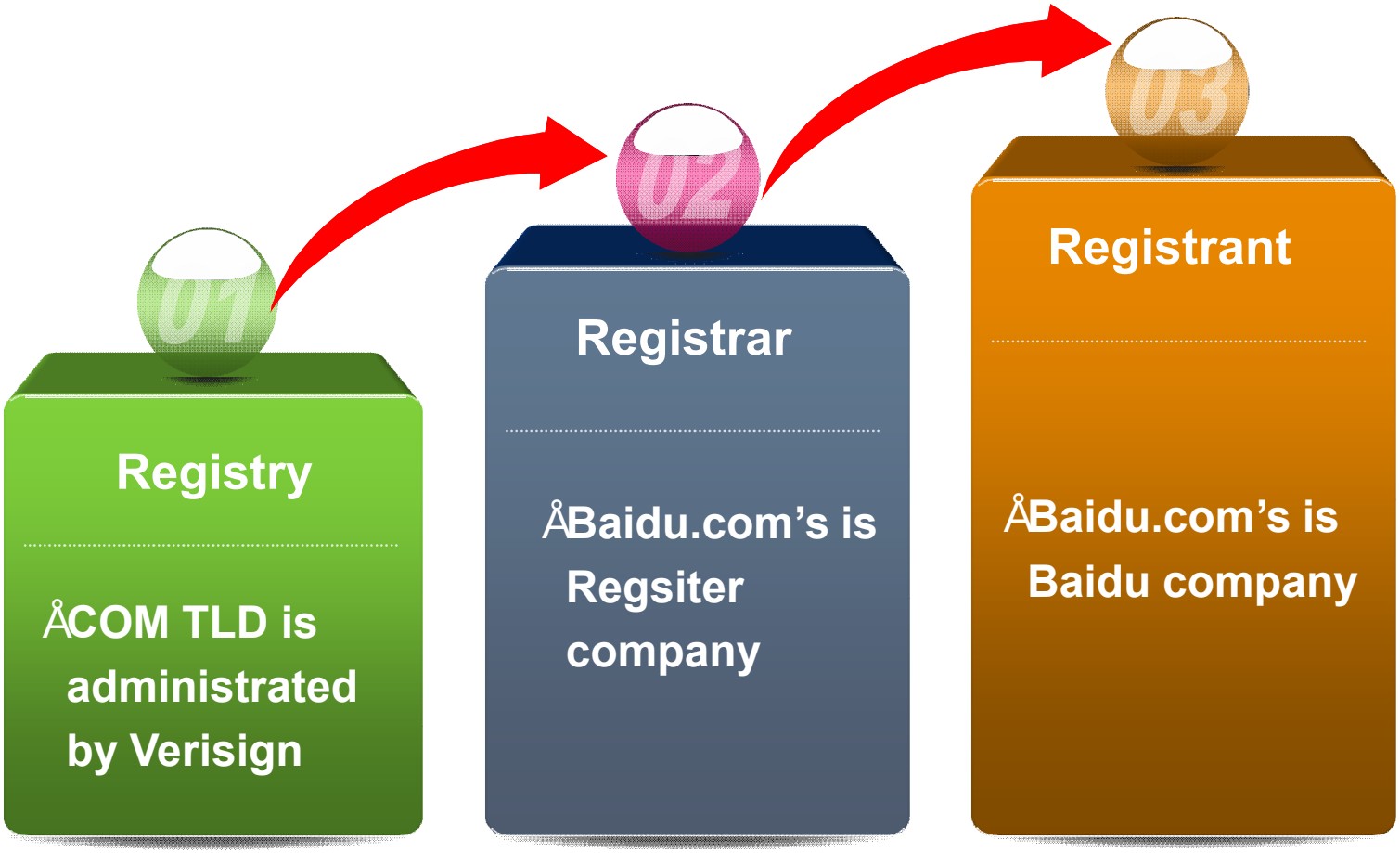
- Rollback is performed by register.com to restore to a clean savepoint at the request of Baidu.
- Direct correction of the DNS records was declined due to the claimed limits of authority.

The ISP side:

- Baiduŝs DNS records were manually corrected in the cache of the recursive servers independent of those in the parent name server.
- DNS caching makes the modification take effect without contacting the parent name server.

Thoughts on the cause

Registration procedure problematic?



Thoughts on the cause (cont'd)

What is the most vulnerable point according to Cannikin Law?

- The security level of registry makes it hard for hackers to break into its database.
- The DNS records at the side of registrant are in its own hand, thus intrusion can be promptly and readily detected and countered.
- Registrar's system sometimes fails to be covered by sufficient safeguards, and its remoteness from the direct control of registrant makes the situation even worse.

What shall we do

- Special security protection tailored for some important domains (most heavily and widely requested domains)?
- Enhanced communication between registrant and registrar?
- General accident prevention measures and procedures for the domain name system as a whole?

Discussions