Internet Censorship in China: Where Does the Filtering Occur?

By Xueyang Xu, Z. Morley Mao, and J. Alex Halderman

Roadmap

- Introduction
- Key Questions
- Types of Censorship
- Http State
- Finding AS/IPs in in China
- Mapping Censorship

Introduction

- China has the largest and most complex online censorship system in the world

Scale

- 513 million people use the internet in China.
  - Lots of traffic
  - Lots of censorship

Key Questions

- Where does the filtering occur?
  - At the border?
  - In the backbone?

- Is the censorship done the same way throughout the network?
  - There are several different ISPs

How do they do it?

- Keyword filtering
- IP blocking
- TCP Cutoff
- URL Hijacking

Keyword Filtering

- All requests are run through a keyword filter

- This applies to every part so many websites / subdomains
  - http://www.hotelshongkong.com/
  - http://www.autism-hongkong.com/

IP Blocking

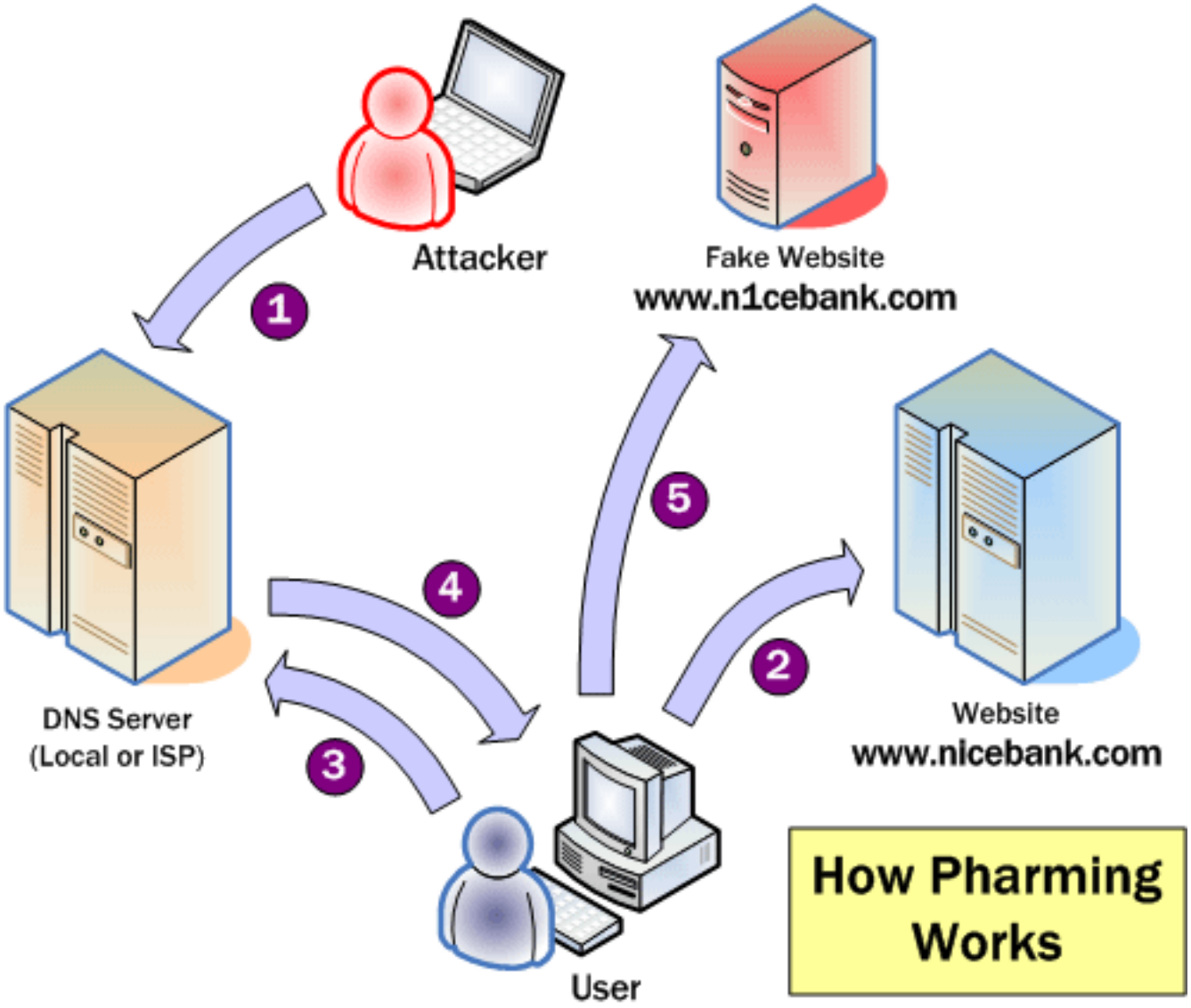
- List of IP addresses that are not allowed
- Easy to thwart by changing IP address / DNS

TCP Cutoff

- Send a TCP RESET flag in the header
- This breaks down the connection
  - Instant reset and stateful reset
    - Instant means you drop the connection
    - Stateful just means you cant jump back into the connection for 150 seconds

URL / DNS Hijacking

- Searches for all A Record DNS queries
- If anything matches the keyword list
  - Return a false IP address that is already blocked


Attacker
Fake Website
www.n1cebank.com
1
DNS Server
(Local or ISP)
5
4
2
3
Website
www.nicebank.com
User
How Pharming Works

HTTP State

- Conflicting results
  - Sometimes GET request itself will not trigger firewall
  - Other times it can
  - This points to different algorithms on different routes

HTTP STATE

- If the firewall is stateful, then the researchers can only connect to HTTP services
- If it is not stateful, then they can just send a keyword to the IP address and see if it gets blocked

AS Level Topology

- Does China filter at the border?
- Do they filter internally?
  - This would allow for domestic filtering
    - Previously thought to not be possible
- How deep does the filtering occur?

Methodology –Find Mapping Between AS and IP

- Find mapping between AS and IP
  - Get list of ASes in China from APNIC
  - Use ROUTEVIEW and RIPE to map
    - Last entry in AS_PATH

This is an Estimation

- Routers can be in the address of a neighboring AS

- APNIC is wrong / inaccurate sometimes

Results From Mapping

- 408,688 AS-pre fix mappings
- 11,824 are in China's address space.
- In 136 AS numbers assigned to China, found 76

Methodology – Get Peerings Between China and Other Countries

- Trace route from worldwide Planetlab to 76 China Ases
- Take the first IP in the AS to ping
- Each hop is checked to see if it is a Chinese / border/internal AS

Results

- 138 internal, 24 border and 92 external Ases

Table 1. Chinese ISP with most number of unique peerings to foreign AS

ISP	AS Numbers	Peerings
CHINANET	4134, 4809, 4812, 23724, 17638	62 (46.6%)
CNCGROUP	4837, 9929, 17621, 4808	23 (17.3%)
TEIN	24489, 24490	8 (6.0%)
CNNIC	37958, 24151, 45096	8 (6.0%)
CERNET	4538, 4789	9 (6.8%)
Other	9808, 9394, 4847, 7497, 9298, 23911	23 (17.3%)

Results

- 5 Ases don’t connect to internal ASes at all
  - Probably an error on the researchers part
- China peered with 20 foreign countries
  - Most with US

AS Hierarchy

- Border AS are parent
- Children are internal
  - Only 2 levels deep – “Backbone” architecture
  - Most of the internal ASes (87.0%) are within direct reach of border ASes

Website Probes

- Finding location of filtering devices
- Top websites are hosted in big cities
- Hand picked 1594 geographically diverse websites

Algorithm

- Send known keywords to each website with increasing TTL.
- Each further step rules out that the firewall is at that level
- Record RESET commands

Results

- 495 router interfaces have filtering
- Most on the border
  - ~3% internal AS (probably error)

Table 2. ASes that contain filtering devices

AS Number	AS Name	Number of Filtering Interfaces
Border ASes		481
4134	CHINANET-BACKBONE	374
4812	CHINANET-SH-AP	9
4837	CHINA169-BACKBONE CNCGROUP	82
9929	CNCNET-CN	4
4538	ERX-CERNET-BKB	4
9808	CMNET-GD	5
9394	CRNET	3
Non-border ASes		14
23650	CHINANET-JS-AS-AP	4
17785	CHINATELECOM-HA-AS-AP	4
37943	CNNIC-GIANT	3
38356	TIMENET	1
17633	CHINATELECOM-SD-AS-AP	1
4813	BACKBONE-GUANGDONG-AP	1

Results

- only 49 of 374 belong to the backbone of CHINANET
  - The rest are provincial
- 80% of 21 provinces that CHINANET serves [12] do their own filtering

- CHINANET filters on the provincial network
- CNCGROUP filters on the backbone
  - 90% of filtering devices belongs to the backbone of CNCGROUP