

# Web安全技术

Web Security

## 1.1 绪论

刘奇旭

liuqixu@iie.ac.cn

中科院信工所 第六研究室



中国科学院大学  
University of Chinese Academy of Sciences

# 一章一问

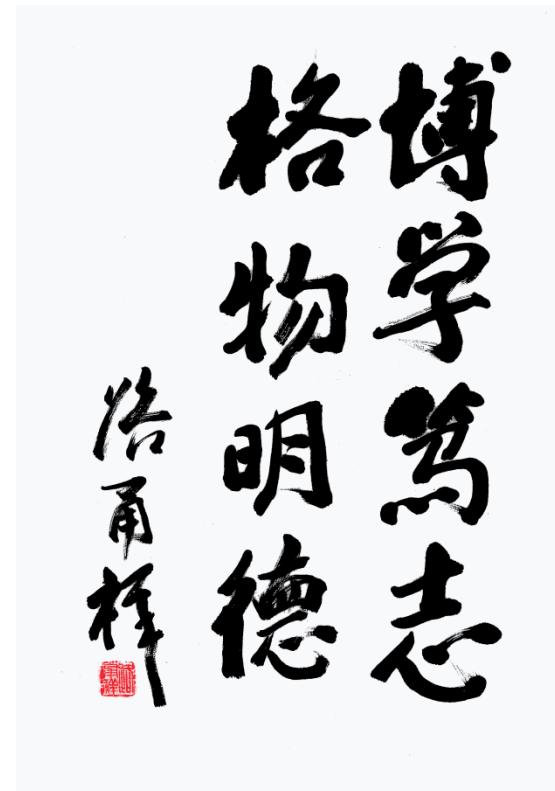
## □Web安全的体系结构？



# 本章大纲

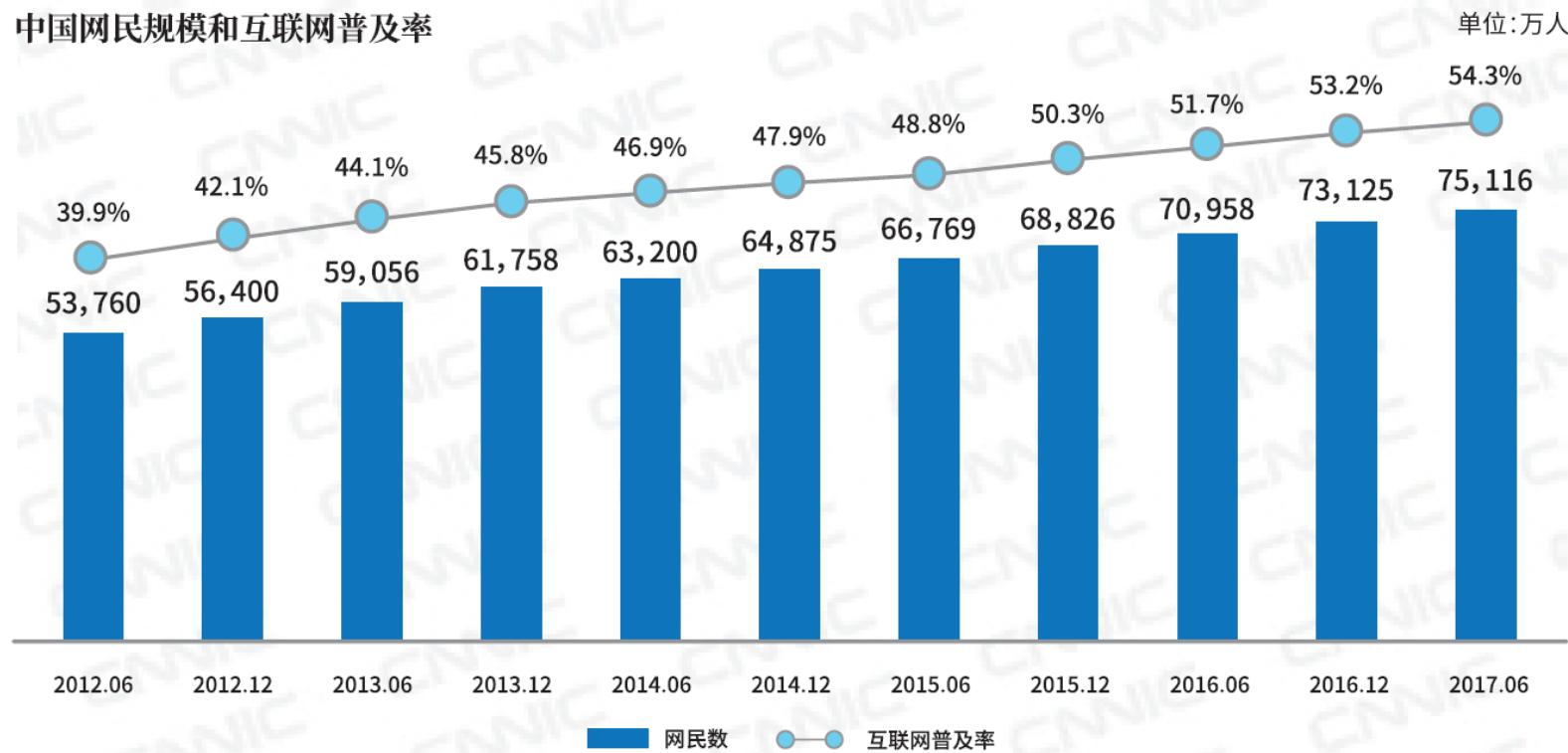
□网络安全现状

□Web安全体系结构



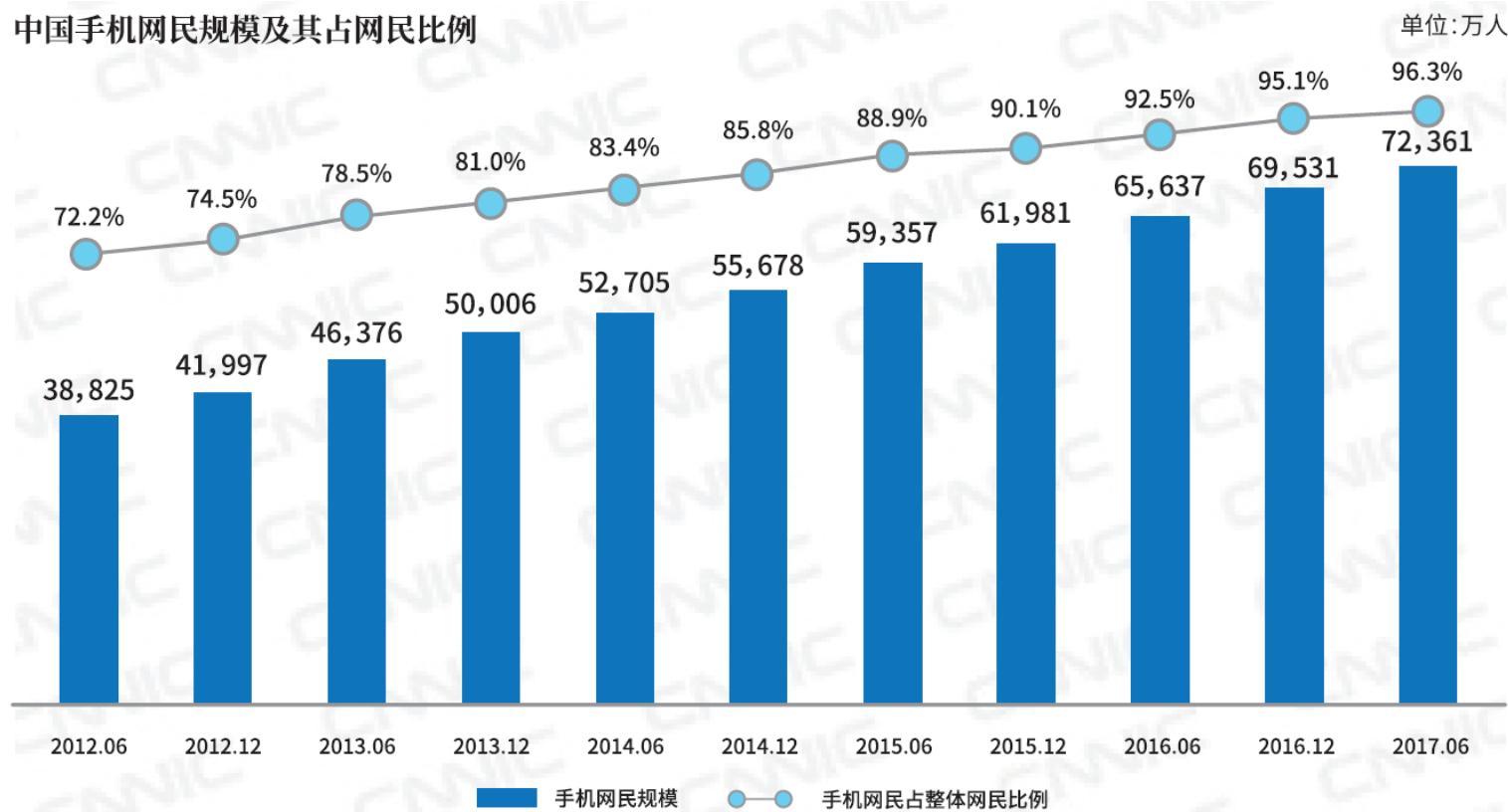
# 2017互联网普及率

- 截至2017年6月，中国网民规模达7.51亿，半年共计新增网民1992万人。
- 互联网普及率为54.3%，较2016年底提升了1.1个百分点。



# 手机上网

- 截至2017年6月，我国手机网民规模达7.24亿，较2016年底增加2830万人。
- 网民使用手机上网的比例由2016年底的95.1%提升至96.3%



以前人们在演唱会上跳舞；如今他们拍视频、  
发“朋友圈”、与好友分享……

1990s



2010s



# 全民自拍狂? SELFIE OBSESSED?



[http://language.chinadaily.com.cn/2016-09/27/content\\_26912396.htm](http://language.chinadaily.com.cn/2016-09/27/content_26912396.htm)

# 中国网民互联网应用使用率

应用	2017.06		2016.12		半年增长率
	用户规模(万)	网民使用率	用户规模(万)	网民使用率	
即时通信	69,163	92.1%	66,628	91.1%	3.8%
搜索引擎	60,945	81.1%	60,238	82.4%	1.2%
网络新闻	62,458	83.1%	61,390	84.0%	1.7%
网络视频	56,482	75.2%	54,455	74.5%	3.7%
网络音乐	52,413	69.8%	50,313	68.8%	4.2%
网上支付	51,104	68.0%	47,450	64.9%	7.7%
网络购物	51,443	68.5%	46,670	63.8%	10.2%
网络游戏	42,164	56.1%	41,704	57.0%	1.1%
网上银行	38,262	50.9%	36,552	50.0%	4.7%
网络文学	35,255	46.9%	33,319	45.6%	5.8%
旅行预订 <sup>3</sup>	33,363	44.4%	29,922	40.9%	11.5%
电子邮件	26,306	35.0%	24,815	33.9%	6.0%

# 中国网民互联网应用使用率（续）

应用	2017.06		2016.12		半年增长率
	用户规模(万)	网民使用率	用户规模(万)	网民使用率	
论坛/bbs	13,207	17.6%	12,079	16.5%	9.3%
互联网理财	12,614	16.8%	9,890	13.5%	27.5%
网上炒股或炒基金	6,848	9.1%	6,276	8.6%	9.1%
微博	29,071	38.7%	27,143	37.1%	7.1%
地图查询	46,998	62.6%	46,166	63.1%	1.8%
网上订外卖	29,534	39.3%	20,856	28.5%	41.6%
在线教育	14,426	19.2%	13,764	18.8%	4.8%
网约车	27,792	37.0%	22,463	30.7%	23.7%
网约专车或快车	21,733	28.9%	16,799	23.0%	29.4%
网络直播 <sup>4</sup>	34,259	45.6%	-	-	
共享单车	10,612	14.1%	-	-	

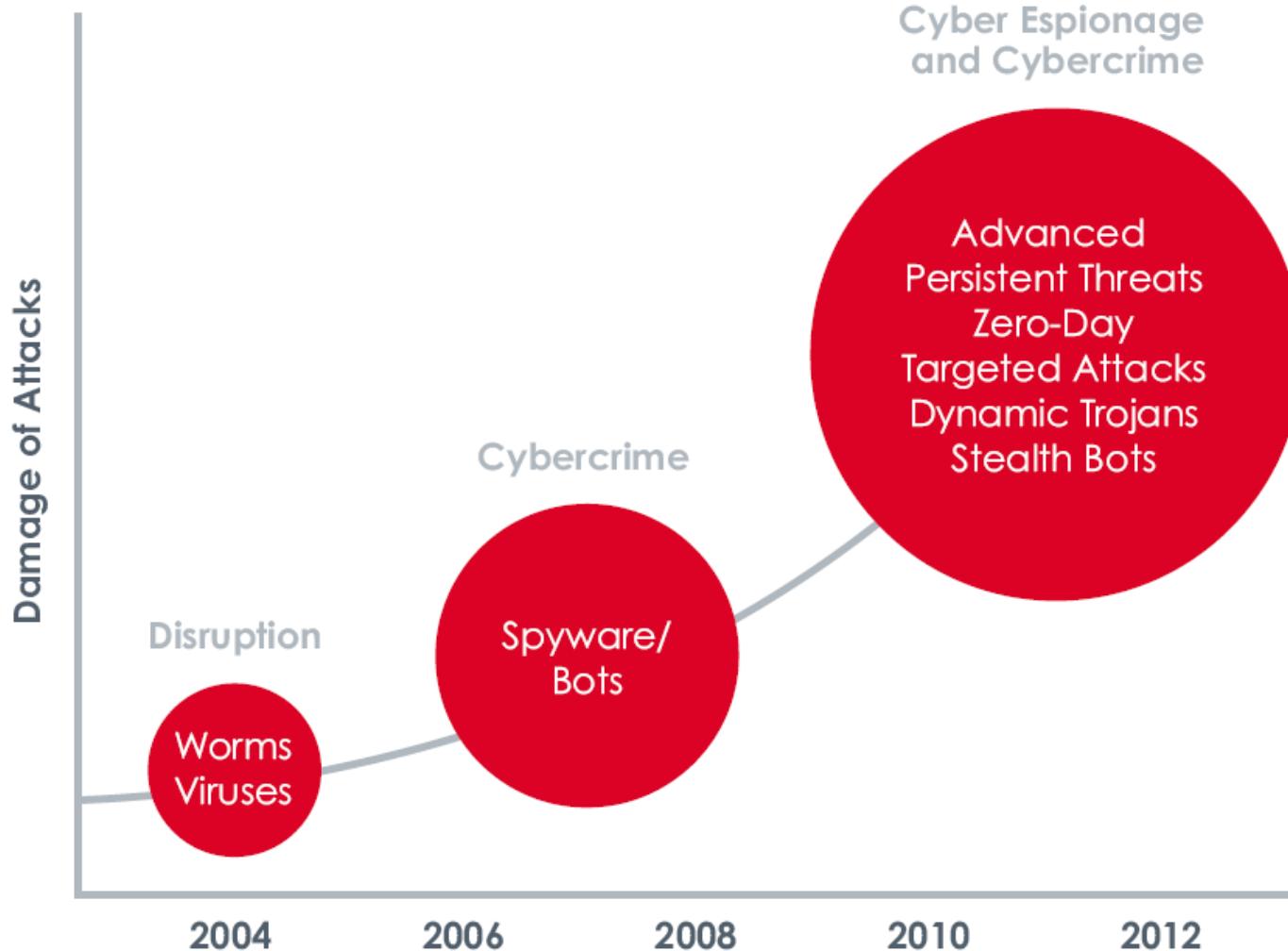
# “土耳其冲突”事件中的互联网媒体

- 土耳其当地时间2016年7月15日晚至16日晨，部分土耳其军人在首都安卡拉和最大城市伊斯坦布尔发动军事政变，迅速控制电视台和电台，并发表声明称已掌控国家政权。
- 正在国内休假的总统埃尔多安，第一时间通过手机视频通话软件FaceTime接受美国有线电视新闻网土耳其语频道（CNN Turk）采访，向全国发表视频讲话，呼吁群众上街反对军队政变。



# 网络安全威胁

## Advanced Persistent Threat



# 极光行动(AURORA)

2010年1月

2010年1月12日，Google称Gmail服务器遭到来自中国的攻击。

搜集Google员工在Facebook、Twitter等社交网站上发布的信息；

利用动态DNS供应商建立托管伪造照片网站的Web服务器，Google员工收到来自信任的人发来的网络链接并且点击，含有shellcode的JavaScript造成IE浏览器溢出，远程下载并运行程序；

通过SSL安全隧道与受害人机器建立连接，持续监听并最终获得该雇员访问Google服务器的帐号密码等信息；

使用该雇员的凭证成功渗透进入Google邮件服务器，进而不断获取特定Gmail账户的邮件内容信息。



# APT1

2013年2月

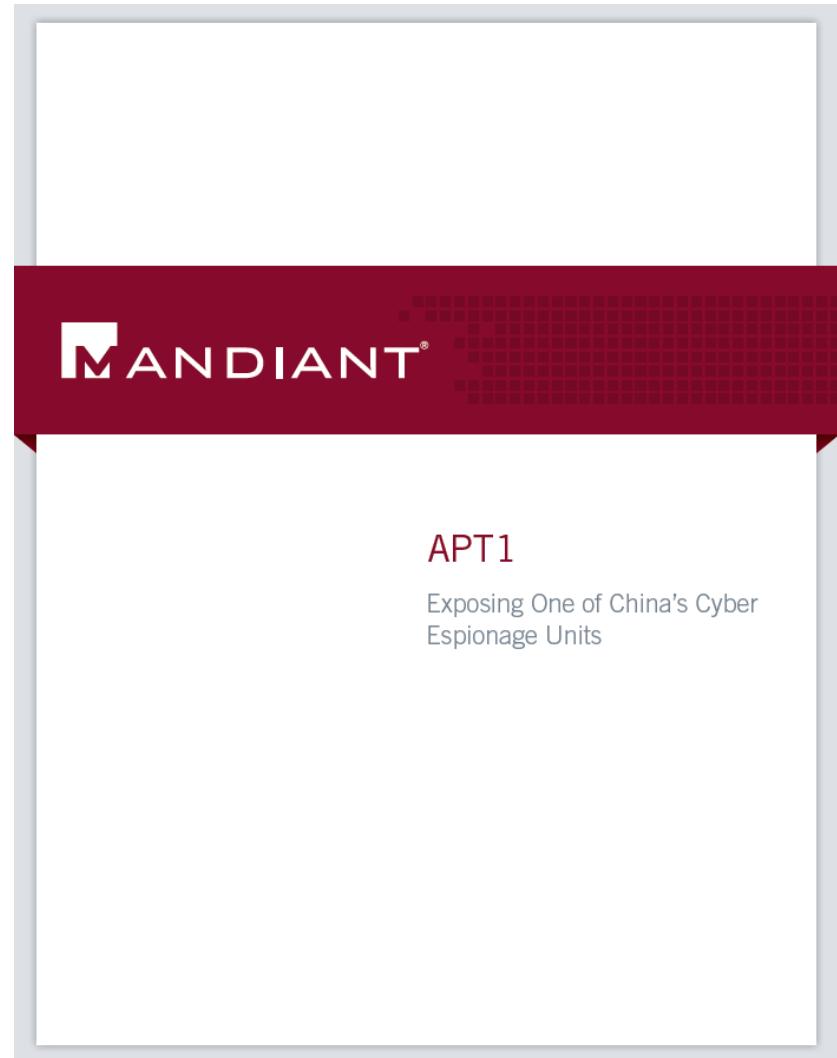
《纽约时报》于2013年2月19日援引美国网络安全公司Mandiant报道称，该公司历时6年追踪141家遭受攻击企业的数字线索，证实实施攻击的**黑客组织**隶属于“**总部设于上海浦东一栋12层建筑内的中国人民解放军61398部队**”。



# APT1

2013年2月

- APT1更倾向于入侵英语为母语的国家的组织；
- APT1发起的1905次入侵中，超过97%发起者使用的是在上海注册的IP地址，并且使用的 是简体中文系统；
- Mandiant揭示了与APT1活动 相关的三个任务角色：  
UglyGorilla、DOTA、  
SuperHard；



# 斯诺登泄漏了多少机密？



爱德华·约瑟夫·斯诺登  
Edward Joseph Snowden

出生日期：1983年06月21日  
美国中央情报局（CIA）前雇员  
博思艾伦咨询公司前员工  
美国国家安全局（NSA）机密泄露者

[查看详细](#)

-  美大规模监控国民隐私
-  欧盟震惊遭美大肆窃听
-  G20峰会成“监听大会”
-  全球38个驻美使馆遭美监控
-  美国入侵中国网络多年

### 个人履历：

#### 青少年：

- ◆ 1983年6月21日出生于北卡罗莱纳州伊丽莎白市
- ◆ 1999年，斯诺登举家搬迁到马里兰州埃利科特市，在那里他在安妮·阿伦德尔社区学院学习计算机专业。

#### 从军：

- ◆ 2004年5月自愿加入美国陆军，数月后在训练中折断双腿被解除兵役。
- ◆ 随后曾在NSA一处隐蔽设施担任警卫。

#### CIA：

- ◆ 担任与信息技术安全有关的职务
- ◆ 2007年被派驻瑞士负责维持电脑网络安全

#### 承包商：

- ◆ 2009年离开CIA，为NSA的私营承包商工作
- ◆ 2013年初到博思艾伦咨询公司工作，职务是在夏威夷一处BSA设施内的系统管理员

#### 泄密：

- ◆ 2013年5月到6月，向媒体泄露NSA的大规模网络和电话监控行为，并自爆身份，引发广泛报道。

### 导语：

“棱镜门”事件持续发酵了一个多月，美国大规模监控国民隐私，欧盟机构和欧盟成员、全球38个驻美使馆、中国等等均遭美国大规模监控。斯诺登好似黑夜里披着斗篷的人权斗士，不断披露美国政府的惊人内幕，以自己无尽渺小的身躯，撼动着美国无尽庞大的权力。



TOP SECRET//COMINT//REL TO USA, FVEY



## JETPLOW ANT Product Data

(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant. JETPLOW also has a persistent back-door capability.

06/24/08



(TS//SI//REL) JETPLOW is a firmware persistence implant for Cisco PIX Series and ASA (Adaptive Security Appliance) firewalls. It persists DNT's BANANAGLEE software implant and modifies the Cisco firewall's operating system (OS) at boot time. If BANANAGLEE support is not available for the booting operating system, it can install a Persistent Backdoor (PBD) designed to work with BANANAGLEE's communications structure, so that full access can be reacquired at a later time. JETPLOW works on Cisco's 500-series PIX firewalls, as well as most ASA firewalls (5505, 5510, 5520, 5540, 5550).

(TS//SI//REL) A typical JETPLOW deployment on a target firewall with an exfiltration path to the Remote Operations Center (ROC) is shown above. JETPLOW is remotely upgradeable and is also remotely installable provided BANANAGLEE is already on the firewall of interest.

2016年8月13日下午5时许，一个自称为“**The Shadow Brokers**”的黑客组织发布声明称：通过对**Equation Group**（方程式黑客组织）的长期跟踪，已成功入侵方程式黑客组织并窃取其所使用的工具集。

- ▶ Firewall
- ▶ BANANAGLEE 针对ASA和PIX,在内存中植入非持久化后门
- ▶ BARGLEE ?针对防火墙的新攻击框架主要是针对Junos的NETSCREEN?
- ▶ BLATSTING 针对Fortinet和TOPSEC的攻击工具
- ▶ BUZZDIRECTION 针对Fortinet攻击工具
- ▶ EXPLOITS 用来做破门的防火墙溢出工具集合
- ▶ OPS 进行攻击行动(OPS)的自动化工具
- ▶ padding ← 未知,怀疑是PIX IOS镜像相关
- ▶ SCRIPTS 攻击过程中的笔记和一些攻击工具的使用方法笔记
- ▶ Shadow-Brokers-ASA.mp4
- ▶ Shadow-Brokers-ASA.webm
- ▶ TOOLS 进行渗透行动(OPS)时所经常用到的工具
- ▶ TURBO ?一个工具集,像是用来做持久化通讯的



# 维基解密泄露CIA文件

2017年3月

- 20170308：泄露Vault7的第一部分YearZero(元年)，大量0day，木马等高度机密资料
- 20170323：Dark Matter入侵苹果Mac和iOS设备的技术与工具
- 20170331：Marble Framework，混淆，伪装成其他国家
- 20170407：Grasshopper，远控木马套件
- 20170411：思科设备的0day（CVE-2017-3881）的细节
- 20170414：Hive（蜂巢），多平台入侵植入和管理控制工具
- 20170421：Wheeping Angel（哭泣的天使），植入三星智能电视的恶意软件
- 20170428：Scribbles，水印，追踪可能被复制的文档
- 20170505：Archimedes，攻击办公室局域网的工具
- 20170512：AfterMidnight，恶意软件植入工具
- 20170519：Athena，针对XP到Win10的恶意工具
- 20170601：Pandemic，针对Windows的持续植入器
- 此处省略更多。。



# 2016年360监测到的APT报告

全球

被攻击目标国家	所属地区	相关报告数量	攻击组织数量	主要被攻击领域
中国	亚洲	26	9	政府、基础设施、教育、科研、大型企业
美国	北美	15	9	政府、金融、基础设施、大型企业
印度	亚洲	15	7	政府、军事、商业组织
俄罗斯	欧洲	15	6	政府、能源、军事、外交、金融
乌克兰	欧洲	14	5	政府、军事、电力、金融
巴基斯坦	亚洲	13	3	政府、军事、外交、能源、教育、科研
伊朗	亚洲	12	3	政府、外交、能源
韩国	亚洲	8	4	政府、大型企业
日本	亚洲	3	3	基础设施、组织机构、大型企业
以色列	亚洲	3	3	政府、军事、金融
土耳其	亚洲	3	2	政府、军事
沙特阿拉伯	亚洲	2	2	军事、金融
埃及	非洲	2	2	政府、军事、金融

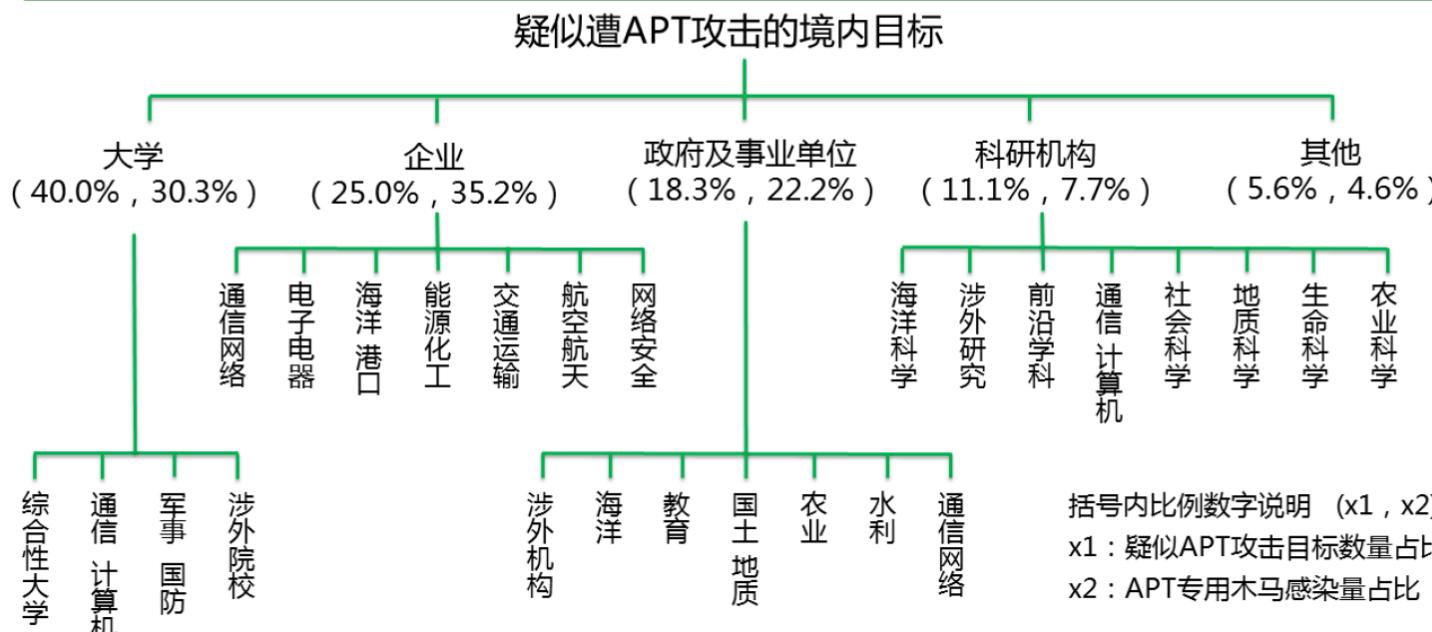


# 全球

排行	APT 攻击领域	攻击组织数量
1	政府、外交	21
2	金融	15
3	大型企业、商业组织、技术组织	14
4	军事、部队、国防	13
5	能源、交通、电力、医疗等基础设施	12
6	特殊个人	3
7	教育、科研	2

# 我国

## 2016疑似APT攻击目标的境内组织机构及相关领域图谱分析



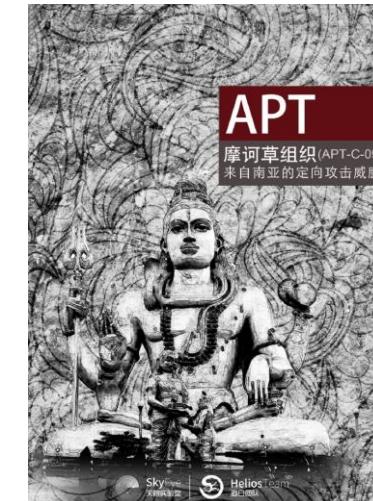
# 以中国地区为目标主要的APT案例

## □ 2016年新披露的

- 摩诃草（hangover、白象）；索伦之眼

## □ 2016年之前

- 海莲花



APT 组织	APT 行动	首先披露报告厂商	最早活动时间	最近活动时间
APT28	APT28	Fireeye	2007 年	2016 年 11 月
APT-C-12	APT-C-12	360	2011 年	2016 年 10 月
OceanLotus (APT-C-00)	OceanLotus	360	2011 年	2016 年 11 月
蔓灵花	蔓灵花	Forcepoint	2013 年	2016 年 11 月
索伦之眼	索伦之眼	Symantec	2010 年	2016 年 8 月
摩诃草	摩诃草	Norman	2009 年	2016 年 11 月

# 网络空间安全理论体系

电子商务安全、电子政务安全、物联网安全、云计算安全等

各种网络空间安全应用技术

应用  
理论体系

芯片安全、操作系统安全  
数据库安全、中间件安全等

通信安全、互联网安全、网络对抗、网络安全管理等

系统安全理论与技术

网络安全理论与技术

技术  
理论体系

网络空间安全体系结构、大数据分析、对抗博弈等

对称加密、公钥加密、密码分析、侧信道分析等

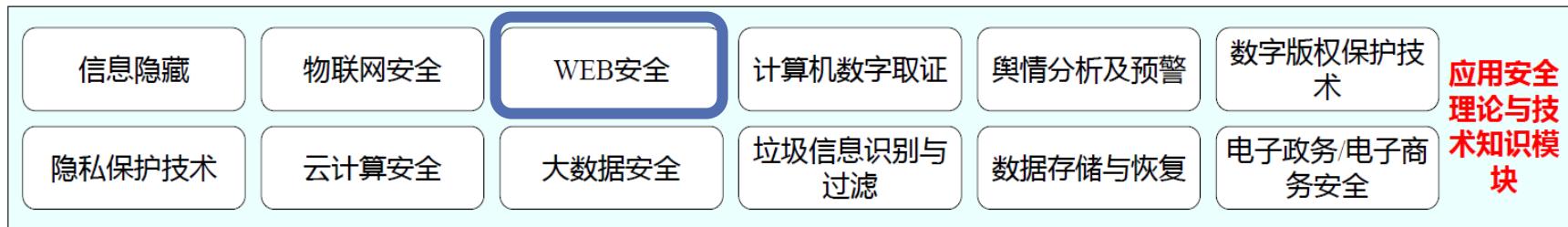
网络空间理论

密码学

基础  
理论体系



# 网络空间安全理论体系（续）



# 什么是“应用”安全？

□ 举例：机密性

Confidentiality

□ 机密性就是防止信息经过某些信息通道被泄露出去。

- 数据机密性服务：使得攻击者想从某个数据项中推出敏感信息是困难的；
- 业务流机密性服务：使得攻击者想通过观察网络的业务流来获得敏感信息是困难的；



# MY HEART IS LOCKED

□ 男主人公向一个心仪的女生表白，她给了一段密文，说解出来了才答应和他约会。

□ ..... - - - - - . . . . . - - - - - . . . . . - - - - - . . . . .

- - - - - . . . . . - - - - - . . . . . - - - - - . . . . .

# MORSE CODE

- 莫尔斯/摩尔斯电码(Morse code)是美国人莫尔斯于1844年发明的，由点（.） 、划（-）两种符号组成：
- 莫尔斯/摩尔斯电码 (Morse code)曾被用在间谍通信，电报，航海信号等各个领域。本质上讲，它只是一种编码，将数字字母等编码为点划序列，适于使用开关电路传输信息



6楼 PorscheL :

首先要把摩斯密码给解开来。  
应该是.

4194418141634192622374.

然后呢?

然后我再想想...

数字的话应该下一步是代入?  
或者是哪个啥



# STEP 1：摩尔斯电码

\*\*\*\*\* / \*---- / ----\*/\*\*\*\*\* /\*\*\*\*\* / \*---- /----\* / \*---- /\*\*\*\*\* / \*---- /-\*\*\*\*\* /\*\*\*\*\* /\*\*\*\*\* / \*----  
- /----\*/\*\*\*\*\* / -\*\*\*\*\* /\*\*\*\*\* /\*\*\*\*\* /\*\*\*\*\* /\*\*\*\*\* /-\*\*\*\*\* /\*\*\*\*\* /

字符	电码符号	字符	电码符号	字符	电码符号	字符	电码符号
0	- - - - -	1	. - - - -	2	. . - - -	3	. . . - -
4	. . . . -	5	. . . . .	6	- . . . .	7	- - . . .
8	- - - . .	9	- - - - .				

□ 4194418141634192622374

# STEP 1：摩尔斯电码

4194418141634192622374

12楼：他——男主人公：

经过昨天一晚的奋斗。

我还是破解不了。

不过今天我死磨她，叫她给提示的后，她说途中有一个步骤是“替代密码”而密码表则是我们人类每天都可能用到的东西。

我会再套多点讯息的..

希望大大帮忙解答阿..

毕竟我也希望不要她亲口说出来这个密码的答案..



# STEP 2

38樓：

数字有偶数个，且注意到41组合出现数次。

于是分组：41 94 41 81 41 63 41 92 62 23 74

注意个位数总是1~4

于是颠倒：14 49 14 18 14 36 14 29 26 32 47

翻成英文字母，前26大写后26小写：NwNRNjNcZfu

然后卡住了.....按大小写分别穷举换位也没看出结果

83樓：翡翠天使

38樓给我的提示。还是让我想到了手机。

你们看解码出来分组后的数字分别是，

41 94 41 81 41 63 41 92 62 23 74

并且每个组合个位数都不超过4。

特别是除了十位数是7和9这两个数字后面有4以外其他的都没有4。



# STEP 2

寻找特征

□ 4194418141634192622374

□ 41多次出现，呈现规律，每两位代表一个字符

□ 41 94 41 81 41 63 41 92 62 23 74

□ 个位数总是1~4

□ 41 94 41 81 41 63 41 92 62 23 74

□ 除了十位数是7和9这两个数字后面有4以外其他的都没有4



# STEP 2

41 94 41 81 41 63 41 92 62 23 74

G Z G T G O G X N C S

中国移动

104楼：熊猫的能

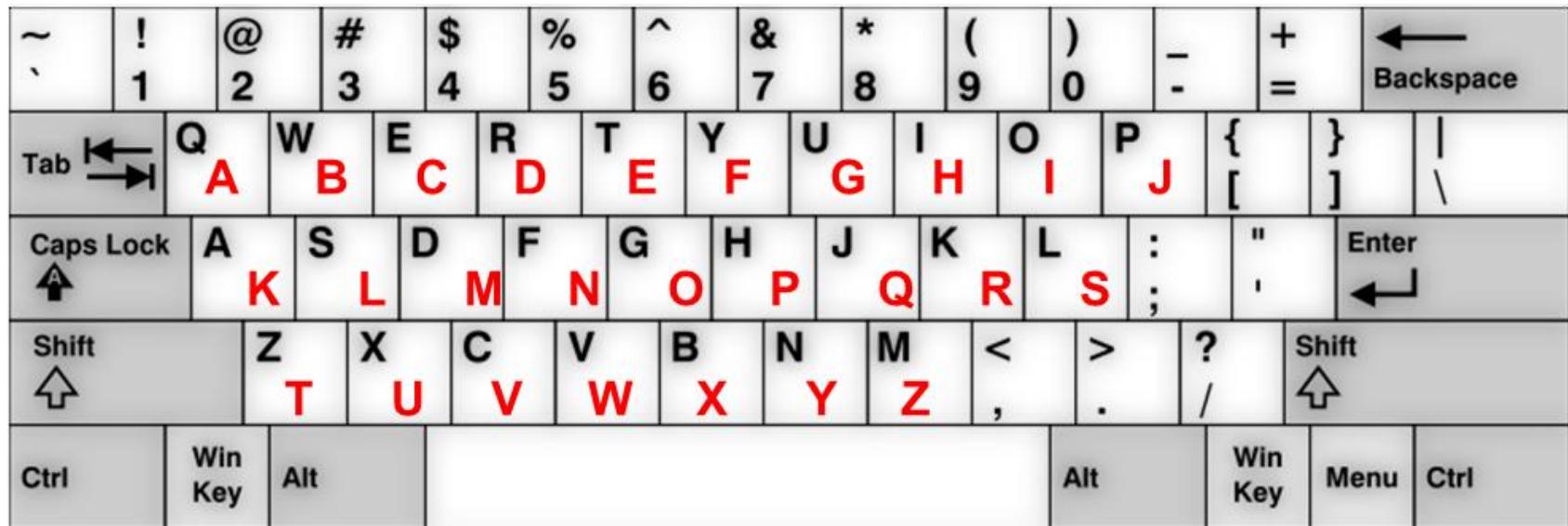
等大家弄出来得哪年了啊。。。

去跟她说，我进不了密码的世界，但我依然想进入你的世界！



# STEP 3

□ G Z G T G O G X N C S



□ O T O E O I O U Y V L



# STEP 4

□ O T O E O I O U Y V L



□ O O T U O Y E V O L I

□ 反序

□ ILOVEYOU TOO

□ I LOVE YOU TOO !

220楼：[HighnessC](#)（主人公——他）

谢过天使了，我有被你感动到。最后的最后你的推理也完全正确。我真的，太感谢你了！



# 回顾

# 密码分析学

□ 41 94 41 81 41 63 41 92 62 23 74



□ G Z G T G O G X N C S



# PHOTO EDITIONS

**O T O E O I**  
**O U Y V L**

# □ I LOVE YOU TOO !

# 代换技术

# 代换技术

# 置换技术

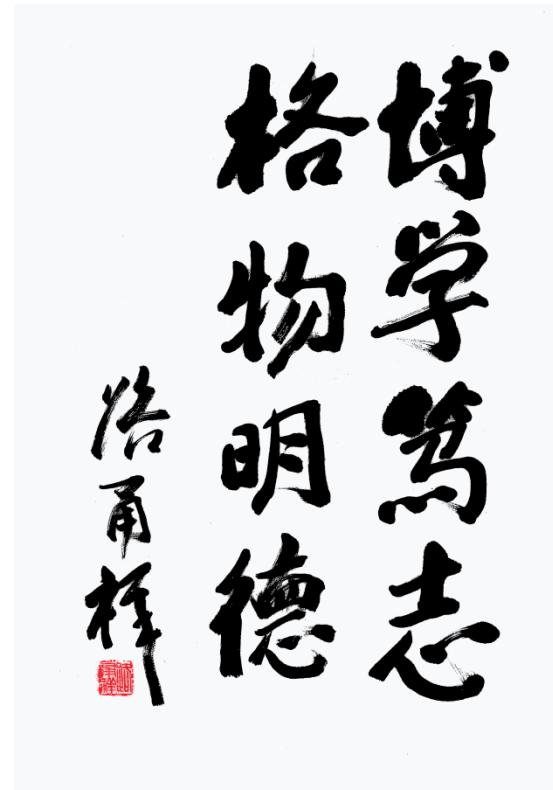
(栅栏技术)

# 密码编码学

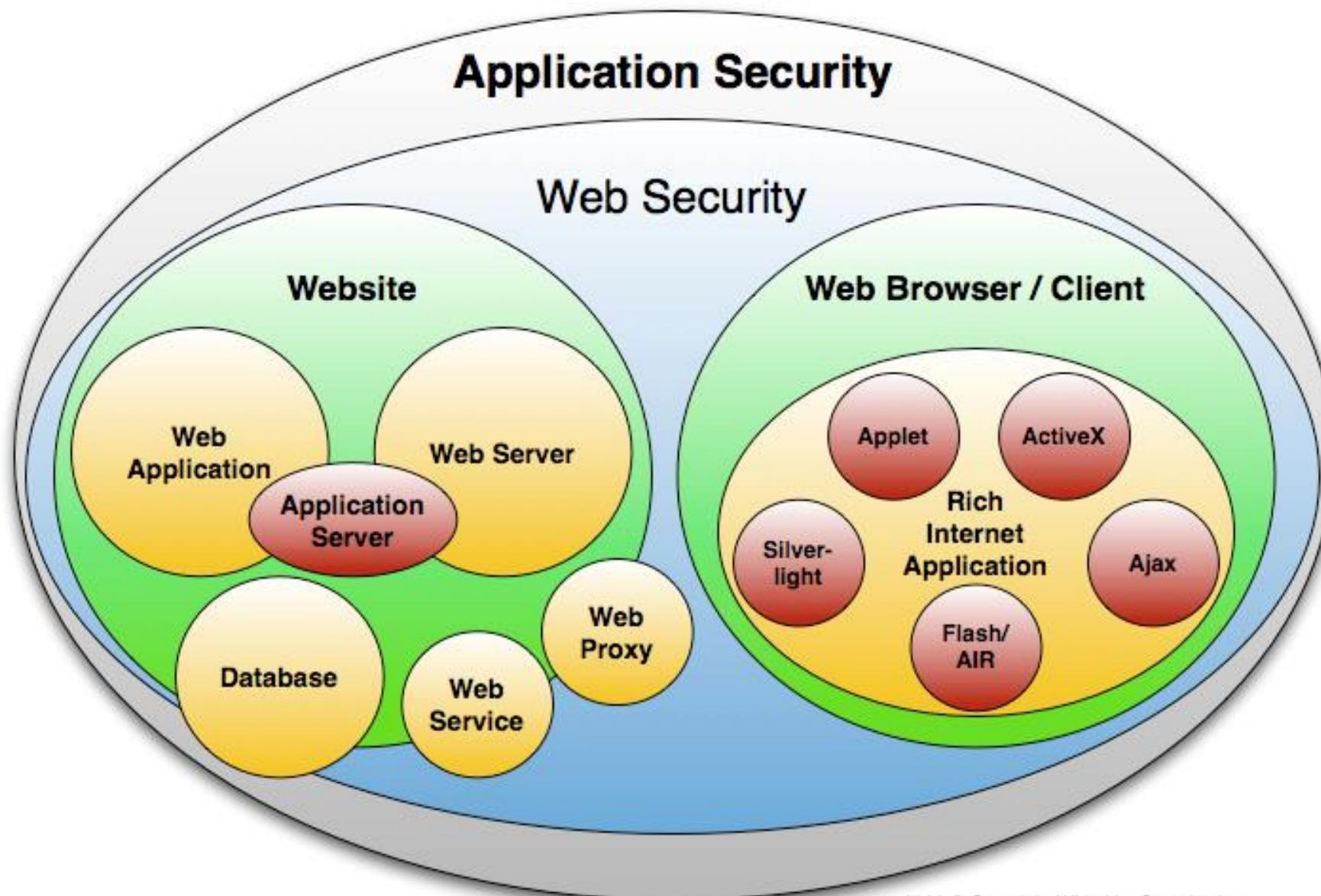
# 本章大纲

□网络安全现状

□Web安全体系结构



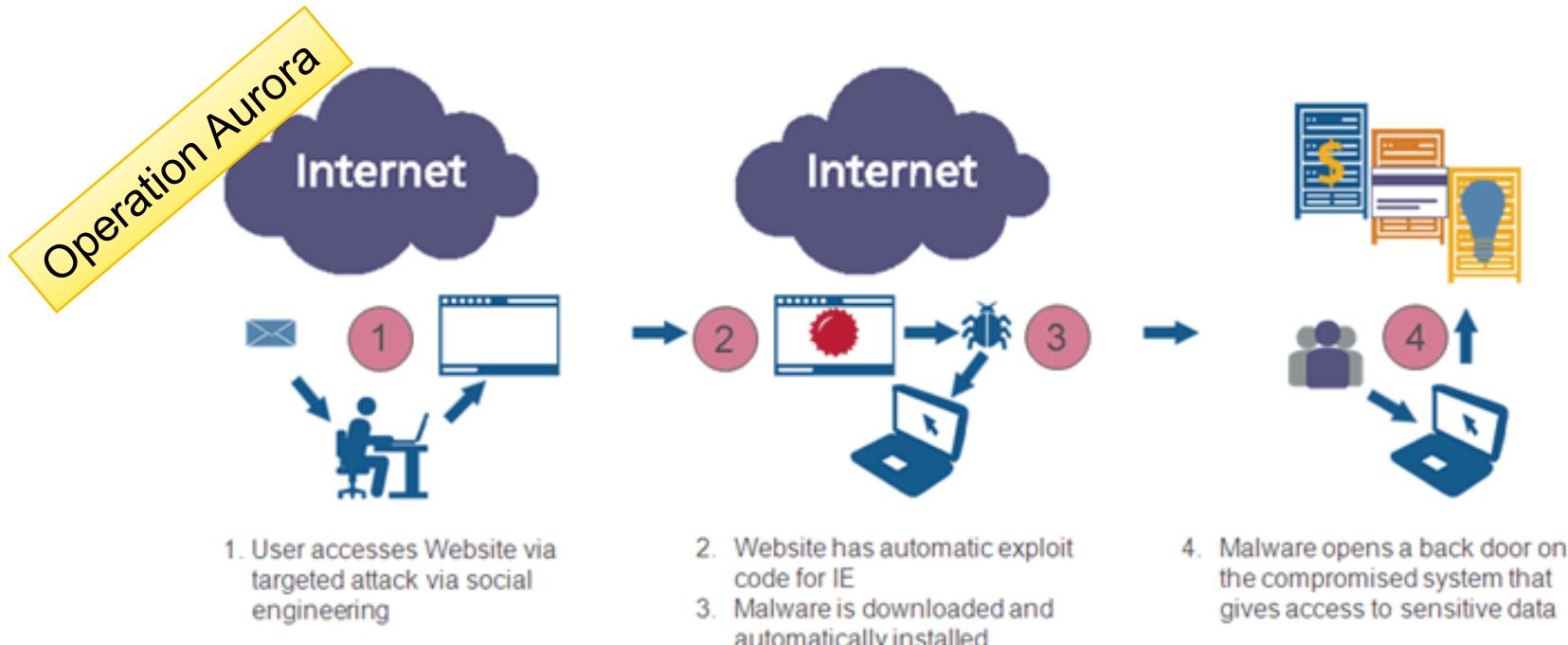
# WEB SECURITY



# APT定向攻击手段

## □ 鱼叉式网络钓鱼（Spear Phishing）

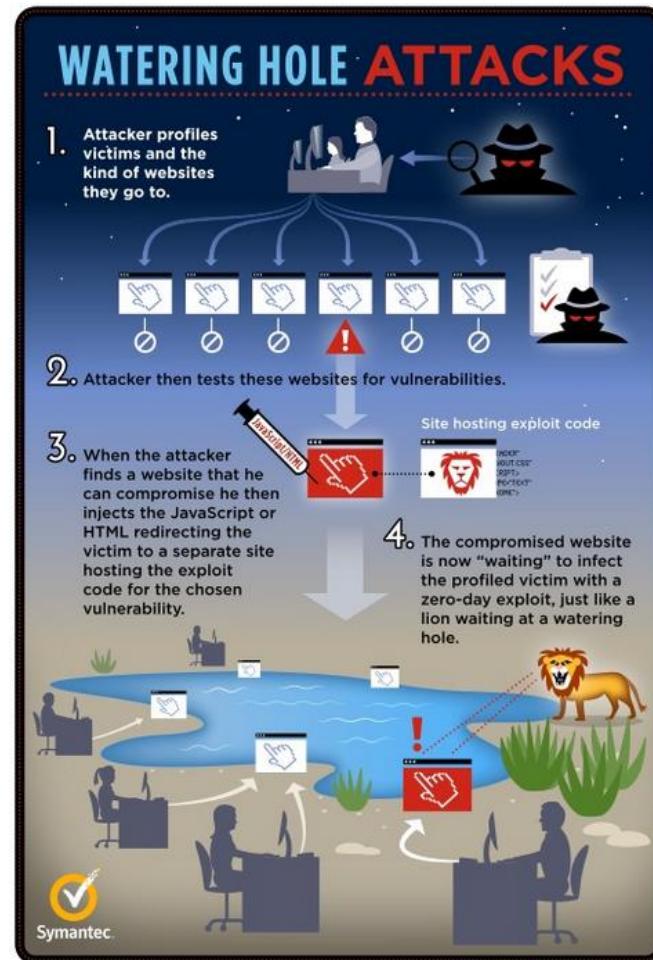
- 在获取目标相关人员的一些信息（比如姓名、电话、账号、密码等信息）的基础上，通过架设钓鱼网站，诱导特定人员访问。
- 原因：访问人员浏览器、Flash插件或Java控件等存在漏洞；



# APT定向攻击手段

## □ 水坑 (Watering Hole)

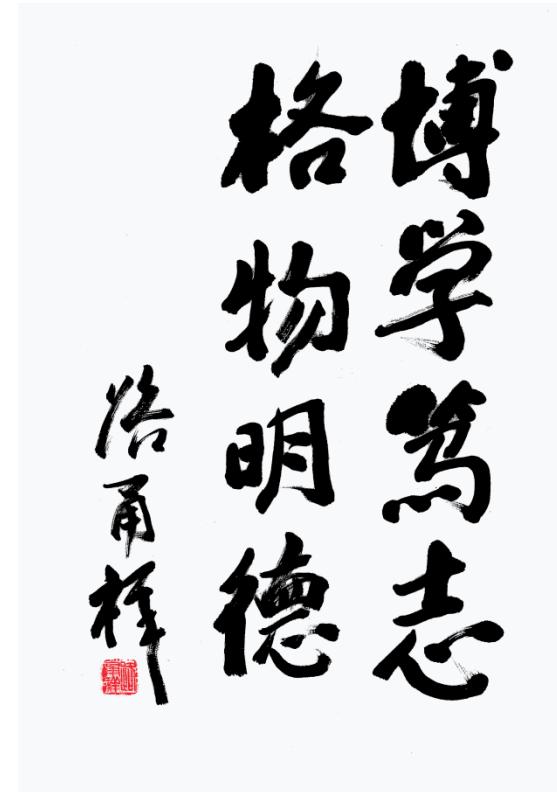
- 通过自行架设或者入侵Web服务站点，在站点中插入恶意的代码，使得受害者在访问这些站点时执行恶意代码；
- 原因：访问人员浏览器、Flash插件或Java控件等存在漏洞；



# 本章大纲

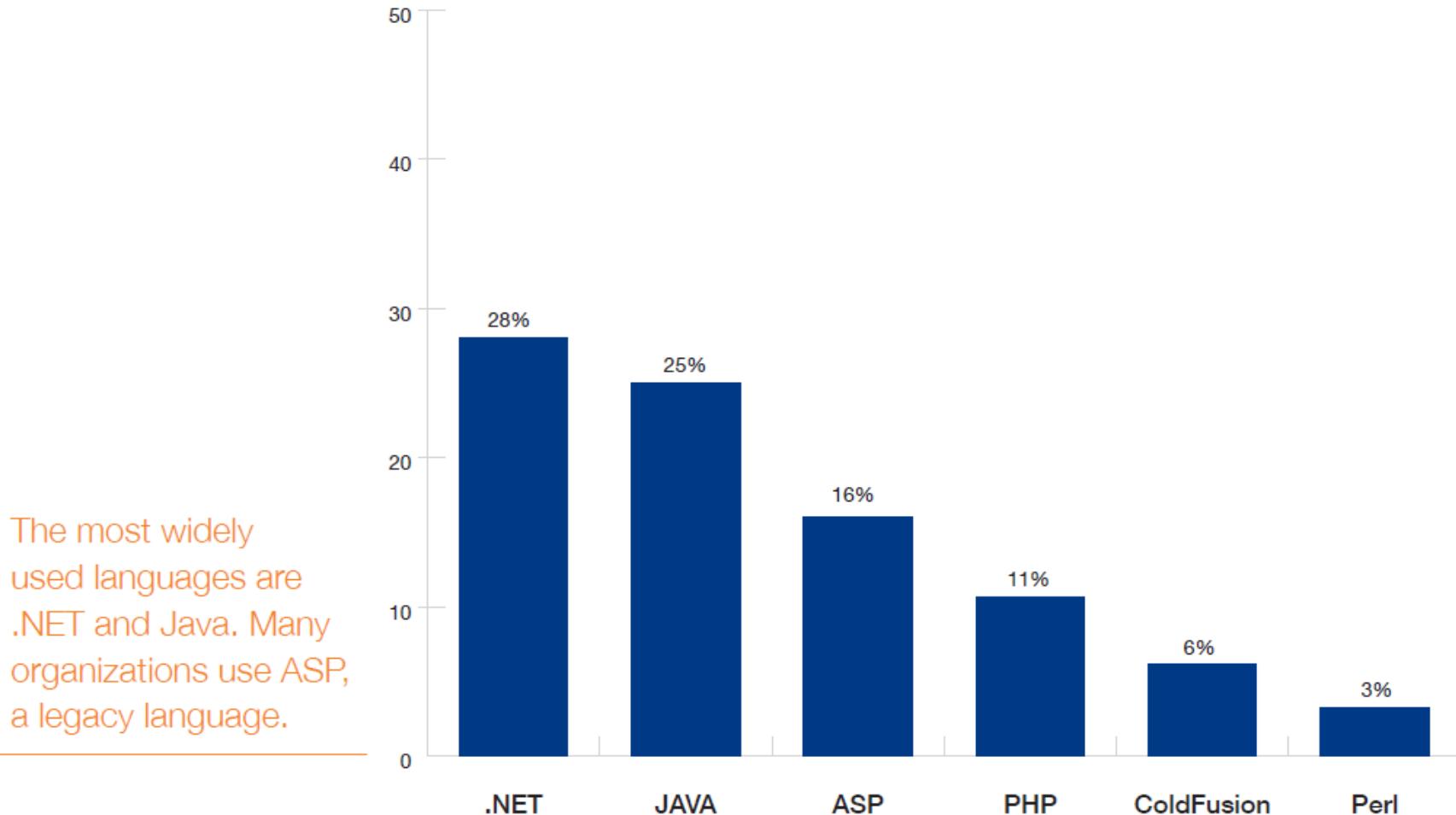
□ 网络安全现状

□ Web安全体系结构



# 网站开发语言

Percent of URLs by language



# WEBSITES

The screenshot shows a browser window with the URL <https://wikileaks.org>. The page is black with white text. At the top, it says "[!] HACKED BY OURMINE [!]" and "# OURMINE #". Below that, it says "YOUR SECURITY IS LOW". The main message reads: "Hi, it's OurMine ( Security Group ), don't worry we are just testing your.... blablablab, Oh wait, this is not a security test! WikiLeaks, remember when you challenged us to hack you?". It also mentions an anonymous tweet and encourages trending on Twitter. The bottom of the page has a red banner with the text "We are Ghost, we never sleep! Dont close your eyes!" and "#OURMINE".

[!] HACKED BY OURMINE [!]

# # OURMINE #

YOUR SECURITY IS LOW

Hi, it's OurMine ( Security Group ), don't worry we are just testing your.... blablablab, Oh wait, this is not a security test! WikiLeaks, remember when you challenged us to hack you?

Anonymous, remember when you tried to dox us with fake information for attacking wikileaks? <https://twitter.com/YourAnonNews/status/679472812013301762>

There we go! One group beat you all! #WikileaksHack let's get it trending on twitter!

[Www.OurMine.Org](http://Www.OurMine.Org) | contact@ourmine.org

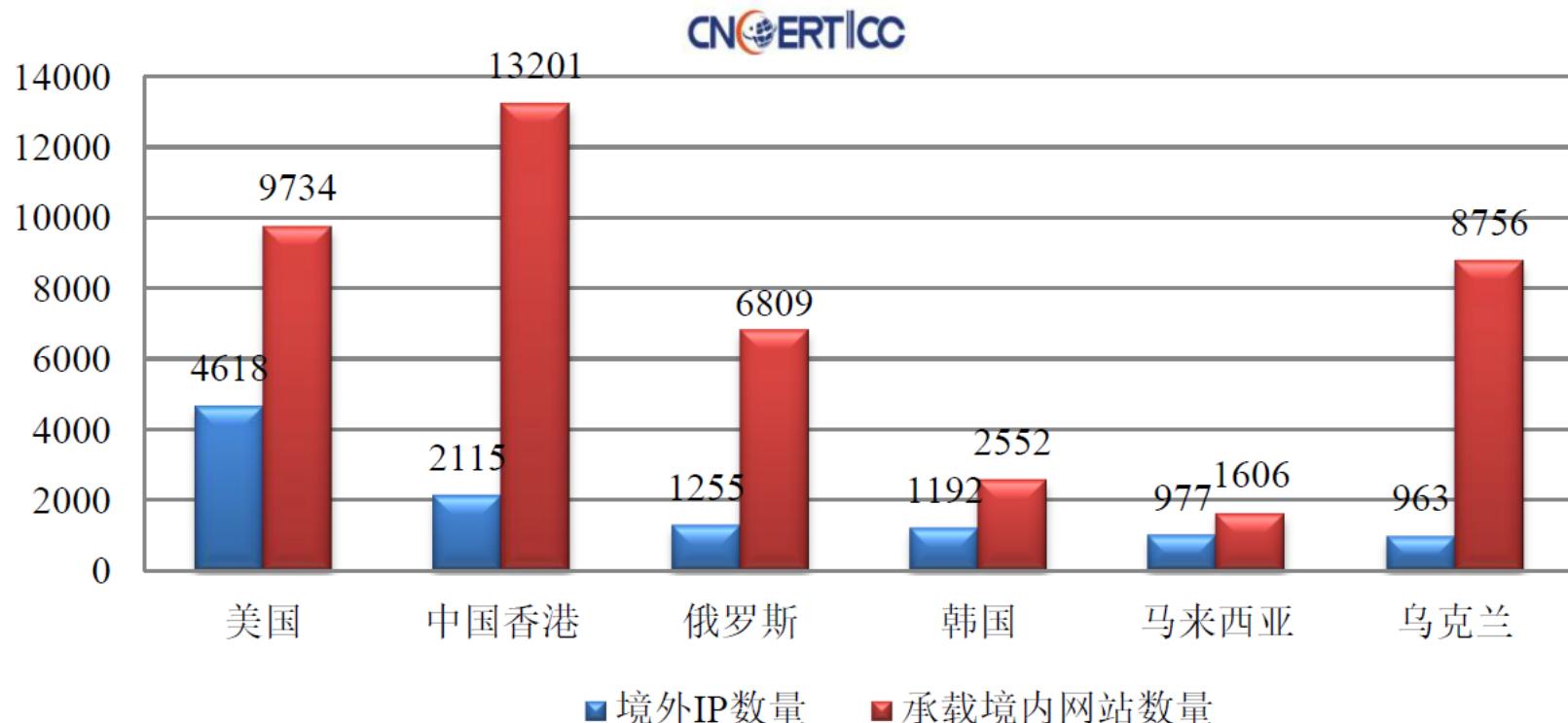
We are Ghost, we never sleep! Dont close your eyes! #OURMINE



# 我国网站安全

□ 2016年，CNCERT监测发现约4万个IP地址对我国境内8.2万余个网站植入后门，网站数量较2015年增长9.3%。

2016年境外向我国境内网站植入后门IP地址所属国家或地区TOP6



Risk exposure does not vary widely between languages, as language choice does not affect number of vulnerabilities.

### Mean number of vulnerabilities in each language



### Vulnerability class by language (percentage)

	ASP	ColdFusion	.NET	Java	Perl	PHP
Cross-Site Scripting	49	46	35	57	67	56
Information Leakage	29	24	44	15	11	17
Content Spoofing	5	4	5	8	6	7
SQL Injection	8	11	6	1	3	6
Cross-Site Request Forgery	2	2	2	4	4	2
Insufficient Transport Layer Protection	0.8	1	0.9	1	0.3	4
Abuse of Functionality	0.3	6	0.3	0.9	0.5	0.2
HTTP Response Splitting	0.9	3	0.8	2	0.8	0.3
Predictable Resource Location	0.1	0.1	0.0	0.2	0.1	1
Brute Force	0.7	0.3	1	2	0.8	1
URL Redirector Abuse	0.7	0.4	0.5	1	1	0.9
Insufficient Authorization	0.2	0.3	0.5	0.9	1	0.2
Fingerprinting	0.3	0.1	0.5	0.6	0.3	0.1
Session Fixation	0.2	0.3	0.2	0.6	0.1	0.3
Directory Indexing	-	-	0.0	0.0	-	0.3

# OWASP Top 10 - 2013 rc1

The Ten Most Critical Web Application Security Risks

A1 – 注入	A1 – Injection
A2 – 失效的身份认证和会话管理	A2 – Broken Authentication and Session Management
A3 – 跨站脚本 (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – 不安全的直接对象引用	A4 – Insecure Direct Object References
A5 – 安全配置错误	A5 – Security Misconfiguration
A6 – 敏感信息泄漏	A6 – Sensitive Data Exposure
A7 – 功能级访问控制缺失	A7 – Missing Function Level Access Control
A8 – 跨站请求伪造 (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
A9 – 使用含有已知漏洞的组件	A9 – Using Known Vulnerable Components
A10 – 未验证的重定向和转发	A10 – Unvalidated Redirects and Forwards



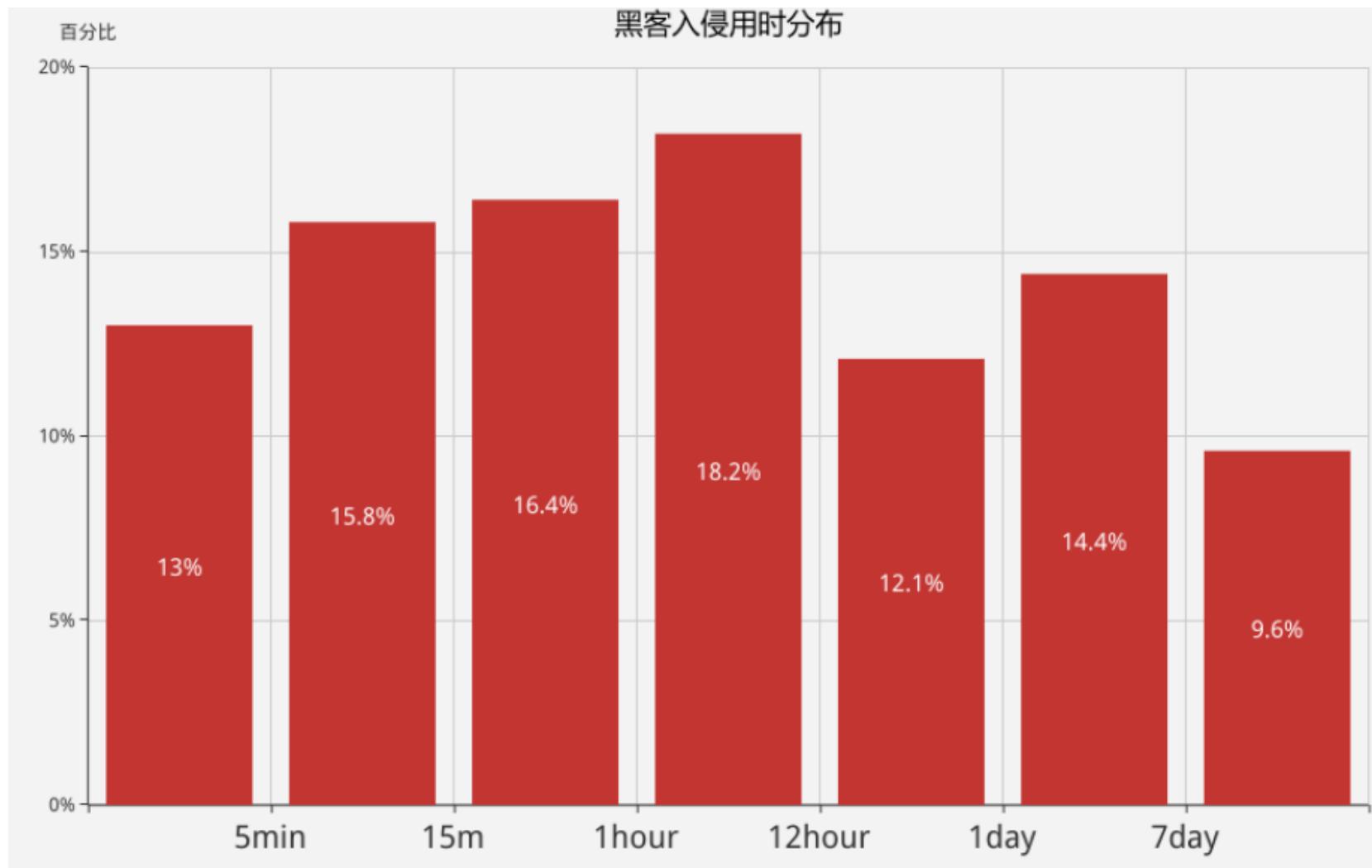
## OWASP Top 10 - 2017 rcl

The Ten Most Critical Web Application Security Risks

OWASP Top 10 – 2013 (旧版)	OWASP Top 10 – 2017 (新版)
A1 – 注入	A1 – 注入
A2 – 失效的身份认证和会话管理	A2 – 失效的身份认证和会话管理
A3 – 跨站脚本 (XSS)	A3 – 跨站脚本 (XSS)
A4 – 不安全的直接对象引用	- 与 A7合并成为 → A4 – 失效的访问控制 (最初归类在2003/2004)
A5 – 安全配置错误	A5 – 安全配置错误
A6 – 敏感信息泄露	A6 – 敏感信息泄露
A7 – 功能级访问控制缺失	-与A4 合并成为 → A7 – 攻击检测与防范不足 (NEW)
A8 – 跨站请求伪造 (CSRF)	A8 – 跨站请求伪造 (CSRF)
A9 – 使用含有已知漏洞的组件	A9 – 使用含有已知漏洞的组件
A10 – 未验证的重定向和转发	A10 – 未受保护的APIs (NEW)



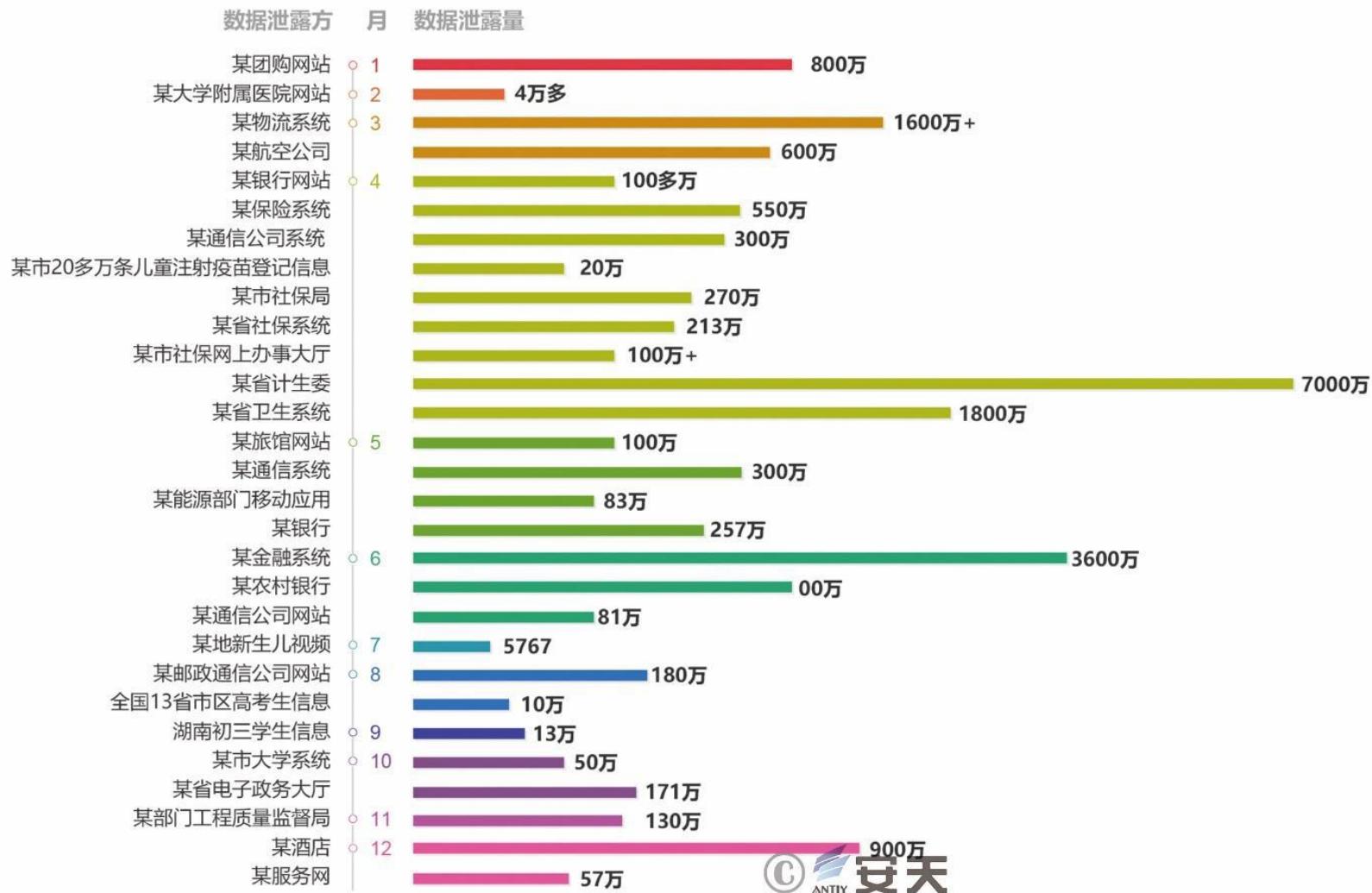
# 黑客入侵用时分布



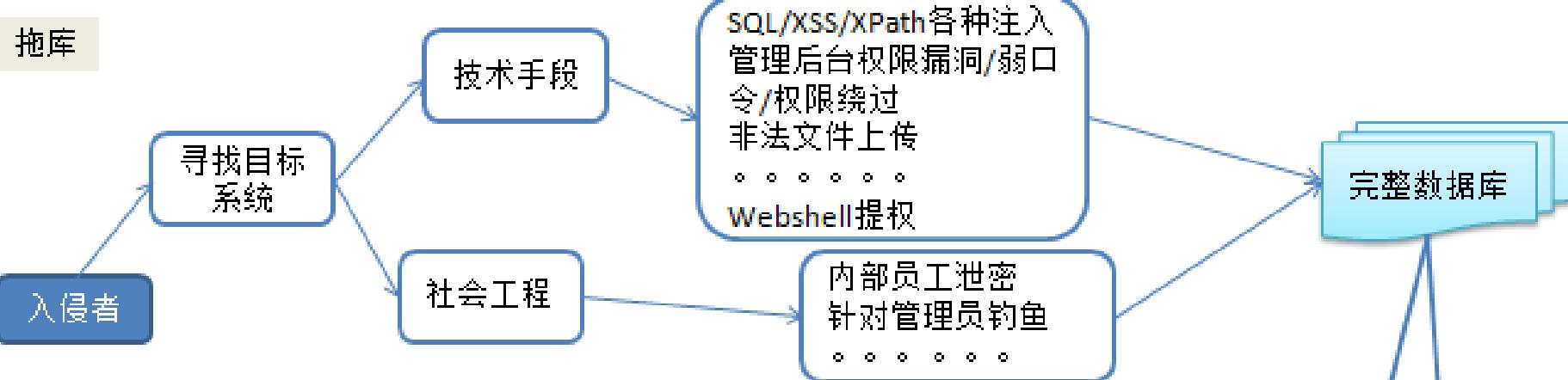
来源:2015年度云盾态势感知报告



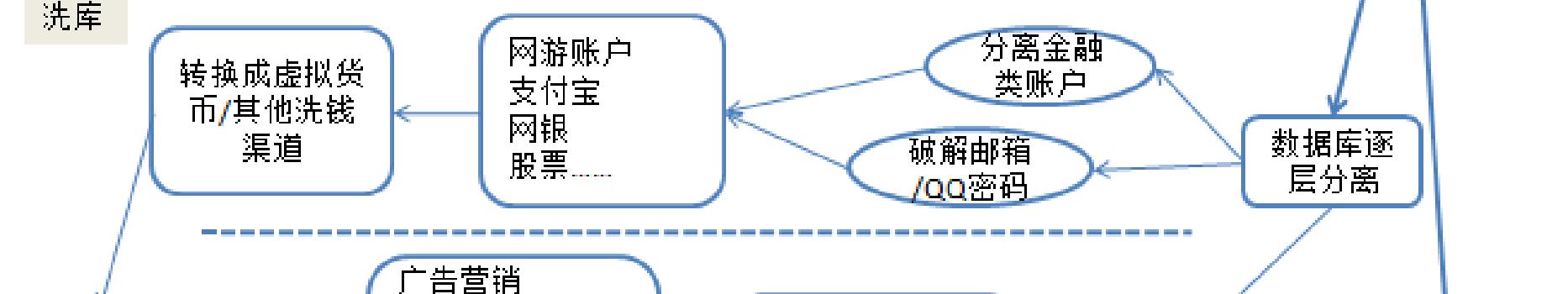
# 2016年重大数据泄露事件



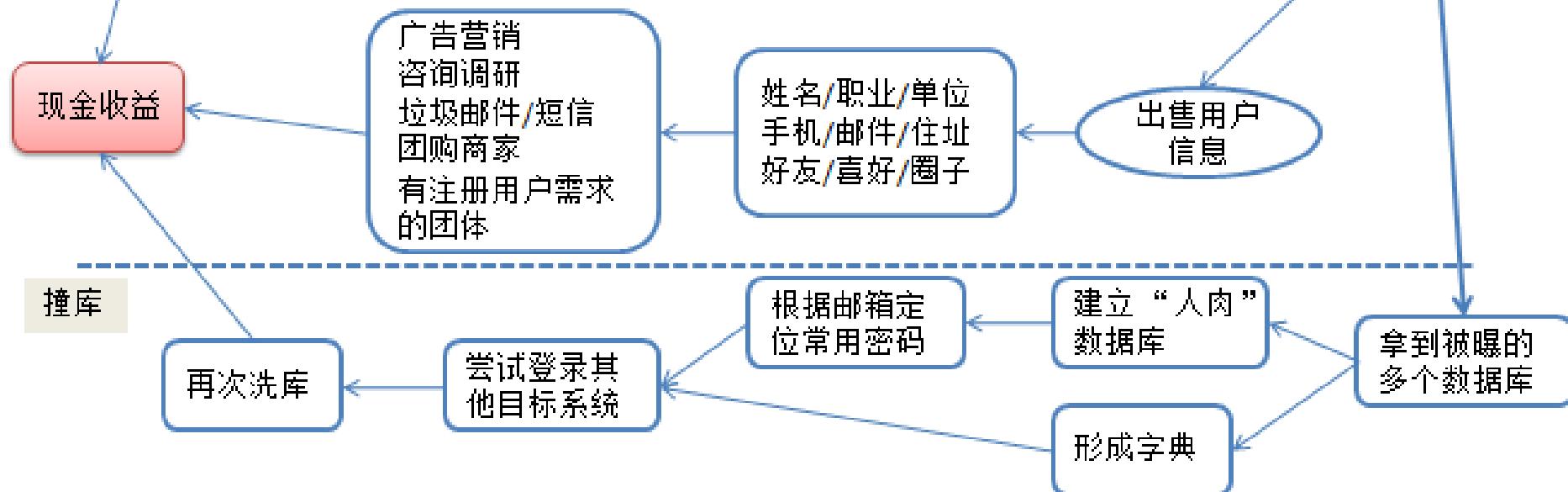
## 拖库



## 洗库



## 撞库



# 信息泄露与网络诈骗

## 个人信息泄露源头

各职能部门泄露源
各金融泄露源
各保险泄露源
各医疗机构泄露源
各房产公司泄露源
各物业公司泄露源
各汽车销售泄露源
各类VIP商户泄露源
各婚庆网站泄露源
各互联网公司泄露源
互联网黑客
...

## 个人信息买卖需求方及直接受益方

各银行业务推广方
各保险业务推广方
各药品、器械推广方
各房地产销售方
各房产中介推广方
各汽车销售方
文化娱乐推广方
各类广告公司
各类公关公司
各类侦探公司
各类违法犯罪个人
...

大量个人信息、隐私数据被出售  
个人获得直接经济利益

利用个人信息从事商业活动  
企业获得直接经济利益

## 间接经济利益受益方

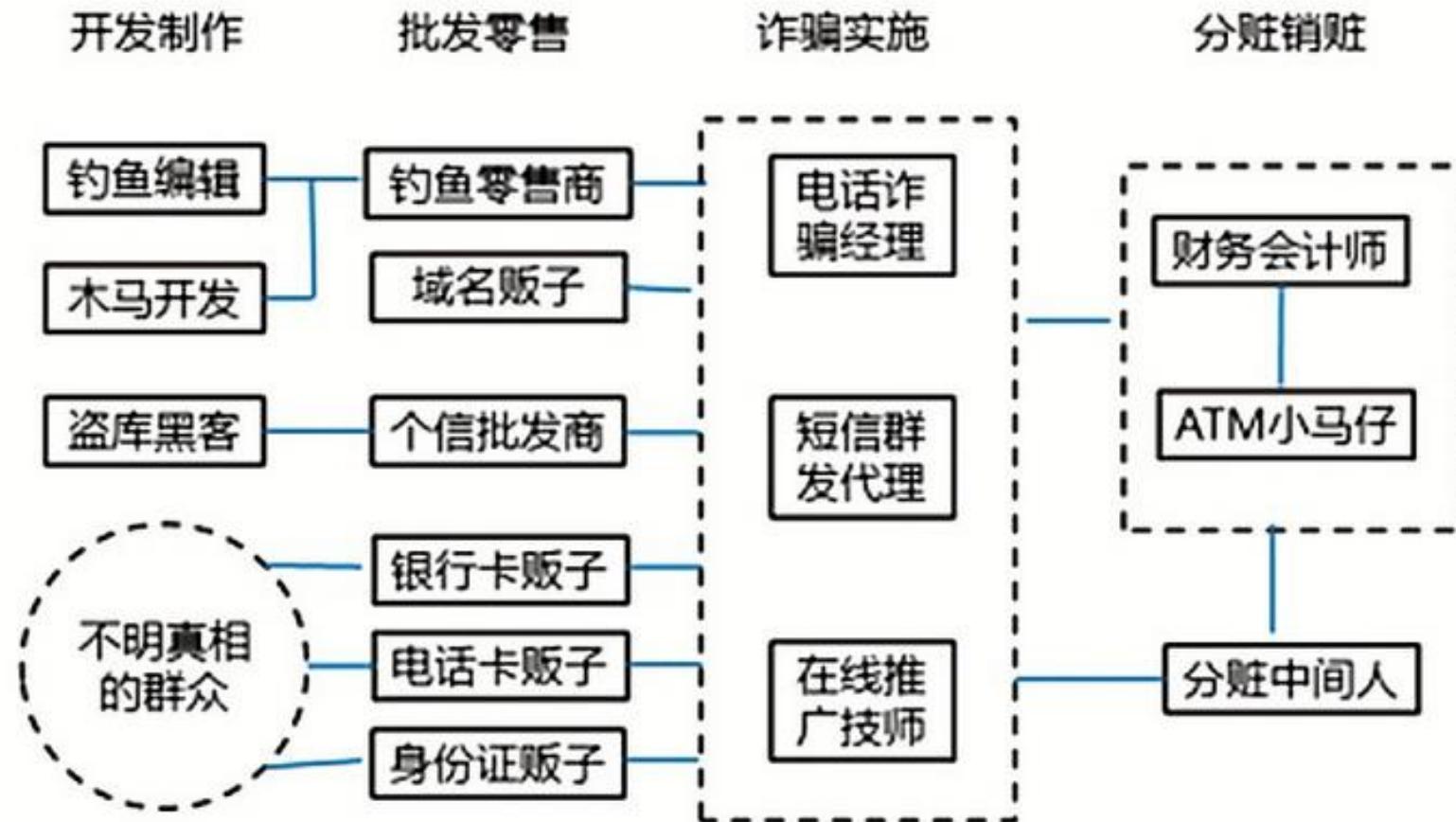
各银行企业
各保险企业
各医疗机构
各房产公司
各汽车销售公司
各类商户
各婚庆企业
各互联网公司
...

完成企业正常生产经营活动  
企业获得直接经济利益



# 网络诈骗

## 现代网络诈骗产业链分工体系



# 网络诈骗

## 徐玉玉事件

2016年8月，山东临沂女孩徐玉玉以568分的成绩被南京邮电大学英语专业录取，8月21日，因被诈骗电话骗走上大学的费用9900元，伤心欲绝，最终不幸离世。2017年7月19日，主犯陈文辉等7名被告人获刑。

“徐玉玉案”中的19岁“黑客”杜天禹侵犯公民个人信息案于8月24日公开审理并宣判，被告人杜天禹非法侵入山东省2016年普通高等学校招生考试信息平台网站，窃取高考考生个人信息64万余条，其中，向陈文辉出售上述信息10万余条，获利14100余元。在徐玉玉案中，个人信息遭到泄露是造成徐玉玉诈骗致死的重要原因。

19岁黑客杜天禹被指控非法获取公民个人信息罪，被判有期徒刑6年，并处罚金6万元

①杜天禹在测试网站漏洞时获取到山东考生信息，利用网站漏洞获取到权限后，杜天禹在数据库中找到了山东高考考生的信息并将信息下载。

②去年暑期接近尾声的时候，徐玉玉案主犯陈文辉与他取得了联系，在和陈文辉的交易过程中，杜天禹贩卖了十万余条高考考生信息，获利共计一万四千余元。

# 入侵老师邮箱拿到考卷

举例

- 曾通过拨号声音破解360总裁周鸿祎手机号，博得周鸿祎、李开复等互联网大佬的睐。
- 这一次，他似乎玩得更大了：他的一篇名为《如何通过入侵老师邮箱拿到期末考卷和修改成绩》的日志，在人人网上疯狂转发。



# HTTP协议

超文本传输协议  
(Hypertext transfer protocol)

□ 一种详细规定了浏览器和万维网服务器之间互相通信的规则，通过因特网传送万维网文档的数据传送协议。

1. 支持客户/服务器模式。
2. 简单快速：客户向服务器请求服务时，只需传送请求方法和路径。请求方法常用的有GET、HEAD、POST。
3. 灵活：HTTP允许传输任意类型的数据对象。正在传输的类型由Content-Type加以标记。
4. 无连接：无连接的含义是限制每次连接只处理一个请求。服务器处理完客户的请求，并收到客户的应答后，即断开连接。可以节省传输时间。
5. 无状态：HTTP协议是无状态协议。无状态是指协议对于事务处理没有记忆能力。



# COOKIE

## 无状态的HTTP协议

- 缺少状态意味着如果后续处理需要前面的信息，则它必须重传，这样可能导致每次连接传送的数据量增大。
- 为了维持一个特定身份的HTTP会话，就需要在每次通信中维护一个标识身份的令牌：Cookie



# WEB邮箱登陆原理

一旦提交了正确的账户和口令，服务器会返回给用户一个Cookie。持有该Cookie的用户将在一段时间内拥有邮箱的访问权限，而不需要再次输入口令。



邮箱帐号登录      手机号登录

邮箱帐号或手机号  忘记密码了?

密码

十天内免登录 ?  SSL安全登录



# 获取教员的**COOKIE**

## □ 伪造Cookie是件很困难的事儿



A screenshot of a web browser's developer tools showing a large amount of cookie data. The code block contains several lines of JavaScript code, likely demonstrating how to access or manipulate cookies.

```
> document.cookie  
"labse_tpl=labse;  
USER=LASTONE&ENTER%5FTYPE=0&NO%5FEYCM=1&GhJUMP=1&MAXRCPTNUM=15&LANG=default%2feyou%5f=h%5FCN&TOKEN=NHjyr6RBz&DOMAIN=software%2enju%2eedu  
%2ecn&UID=1jk10&LOGIN%5FDOMAIN=software%2enju%2eedu&LOGIN%5FUID=1jk10&ATTSIZE=10485760&EXAMINELEVEL=0&ENABLEEXAMINE=0&CALLBACK=0&TRACEMA  
IL=1&GROUPADDR=0&QUEUESEND=0&COMPANYADDR=0&VIEWLIST=0&GLOBALPERMISSION=0&NOTATION=0&BYTEPERCENT=0&BOOKMARK=0&MOBILEMESSAGE=0&DIALUP=0&VIDEOM  
AIL=0&SECUREMAIL=0&VOICEMAIL=0&CALENDAR=0&STORAGE=0&TOTALSPACE=2000&LOCKSTATUS=0&USERNAME=&EXPTIME=0&LETTERS=2000&QUOTA=2000&TAKEOVERPERMIT=0&  
ENABLENSFBACKUP%5FCLIENT=0&ENABLENSFARCHIVE=0&ENABLENSFBACKUP%5FSERVER=0&SKIN=current&COMPOSE%5FMSG=&COMPOSE%5FFOLDER=&COMPOSE%5FMETHOD=0"
```

## □ 想办法直接获取才是上策

- 使用浏览器内的JavaScript能够获取当前站点的Cookie。
- 邮件系统对用户发送的邮件过滤不足，允许邮件中嵌入脚本代码
- 教员打开包邮件将使得预设的JavaScript代码执行，获取Cookie并发送



# TIMING IS EVERYTHING

- 除非点击了记录密码，否则关闭浏览器的同时，Cookie就会失效，需要在获取了Cookie后马上行动。
- 使用JavaScript获取Cookie，然后发送到远端预设的服务器。服务器使用PHP编写脚本，一旦收到Cookie就立即发到QQ邮箱。利用微信的邮件提醒功能在第一时间得知Cookie到手的信息。



# LET 'S ROCK

## □ 伪造Cookie是一件很困难的事儿

老师您好😊，我是软件学院大三的刘立均是哪几门课，请问如何查看  
谢谢老师>\_\_\_\_<

```
1 
```

## □ 等待，等待

今天 (5 封)					
<input type="checkbox"/>		SE_NJU HACK	new cookie - document.cookie="izstat_uv=25..."	12分钟前	
<input type="checkbox"/>		SE_NJU HACK	new cookie - document.cookie="" ;document.c...	今天 12:59	
<input type="checkbox"/>		SE_NJU HACK	new cookie - document.cookie="!zstat_uv=25..."	今天 11:18	
<input type="checkbox"/>		SE_NJU HACK	new cookie - document.cookie="izstat_uv=25..."	今天 11:16	
<input type="checkbox"/>		SE_NJU HACK	new cookie - document.cookie="!zstat_uv=25..."	今天 11:11	



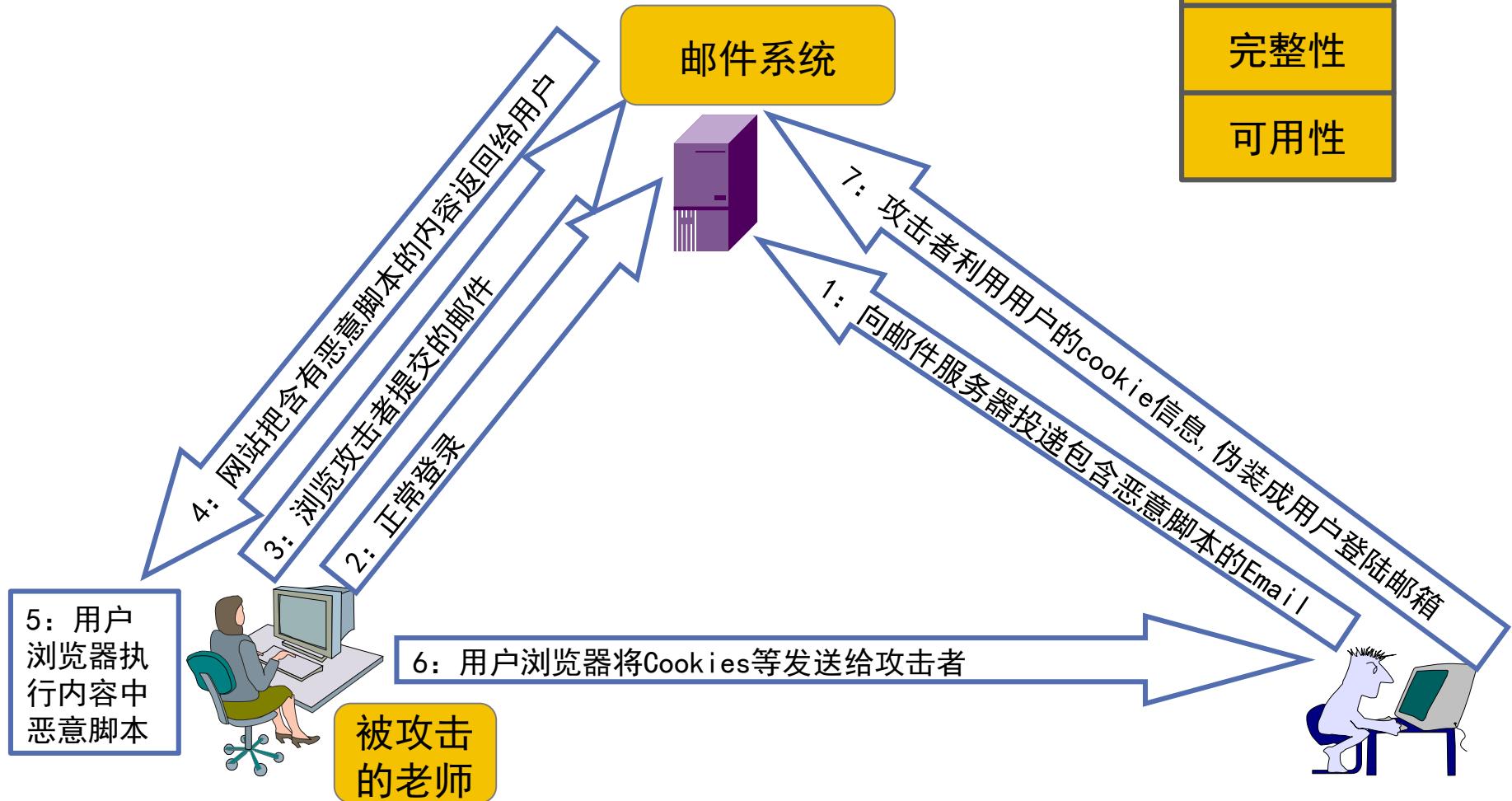
# GOT IT

□ 将获取的Cookie替换掉现有的Cookie

□ 登进了教员的邮箱



# 事件过程回顾



# XSS ( CROSS SITE SCRIPTING )

- XSS是跨站脚本攻击(Cross Site Scripting)。它指的是恶意攻击者往Web页面里插入恶意html代码，当用户浏览该网页时，嵌入其中Web里面的html代码会被执行，从而达到恶意用户的特殊目的。
- 跨站脚本攻击主要是由于Web服务器没有对用户的输入进行有效性验证或验证强度不够，而又轻易地将它们返回给客户端造成的。



# 邮件的故事不是特例

□ 其实很多邮件系统都存在类似问题。



# 中国留学生“黑”教授电脑篡改成绩 在美获刑4年

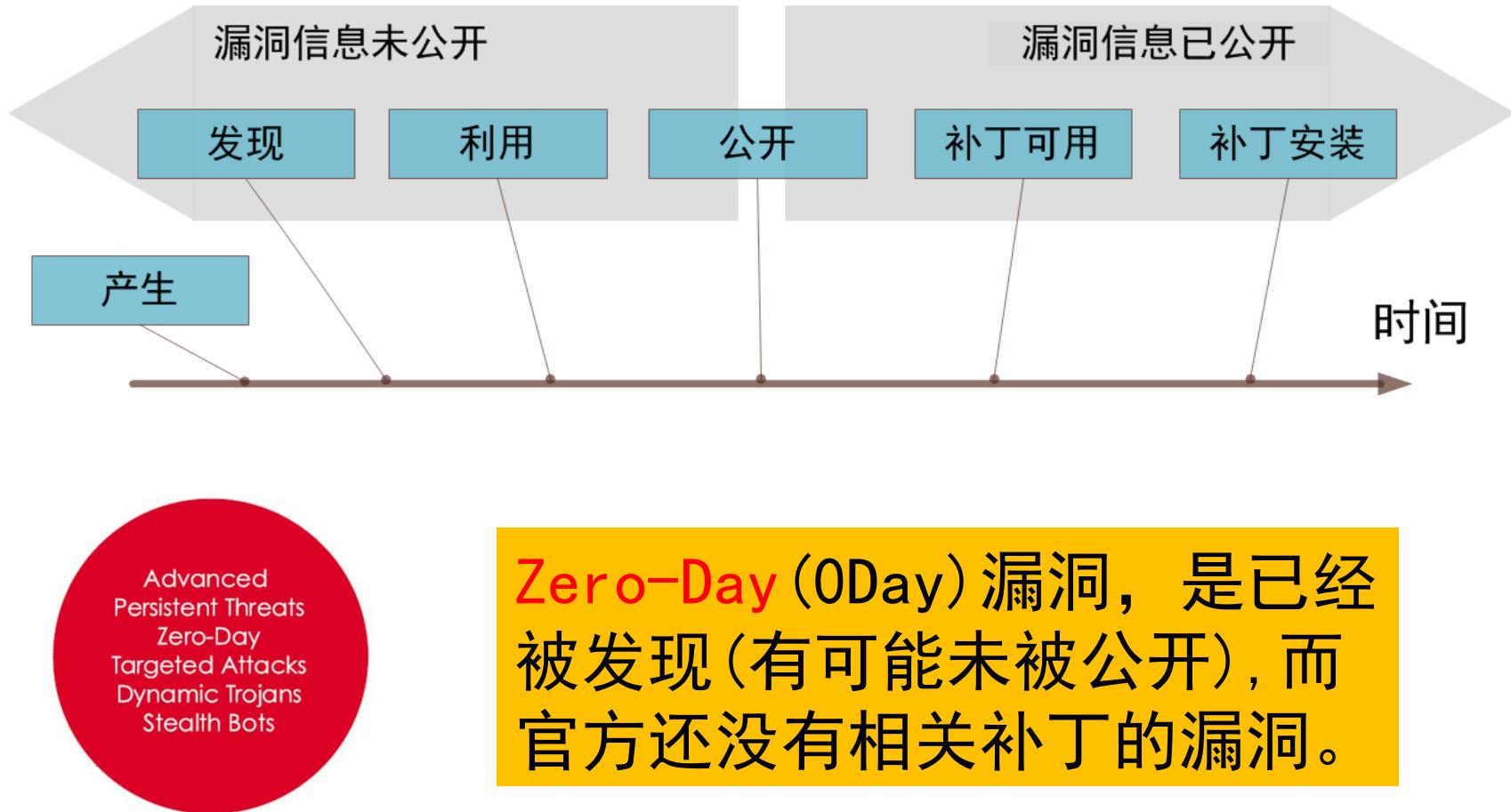
日前，一中国留学（微博）生因“黑”教授电脑篡改成绩，在美获刑4年。据法庭文件显示，孙从2008年5月起便开始入侵电脑篡改成绩，在第四年时被发现。“精明的”的孙超然失去了他在普渡大学的学士学位，还被踢出了波士顿大学的研究所。

据悉，2013年6月13日，普渡大学工程专业学生孙超然被控多次入侵教授电脑并篡改个人成绩，也因此以“优异成绩”从该校毕业进入波士顿大学读研。

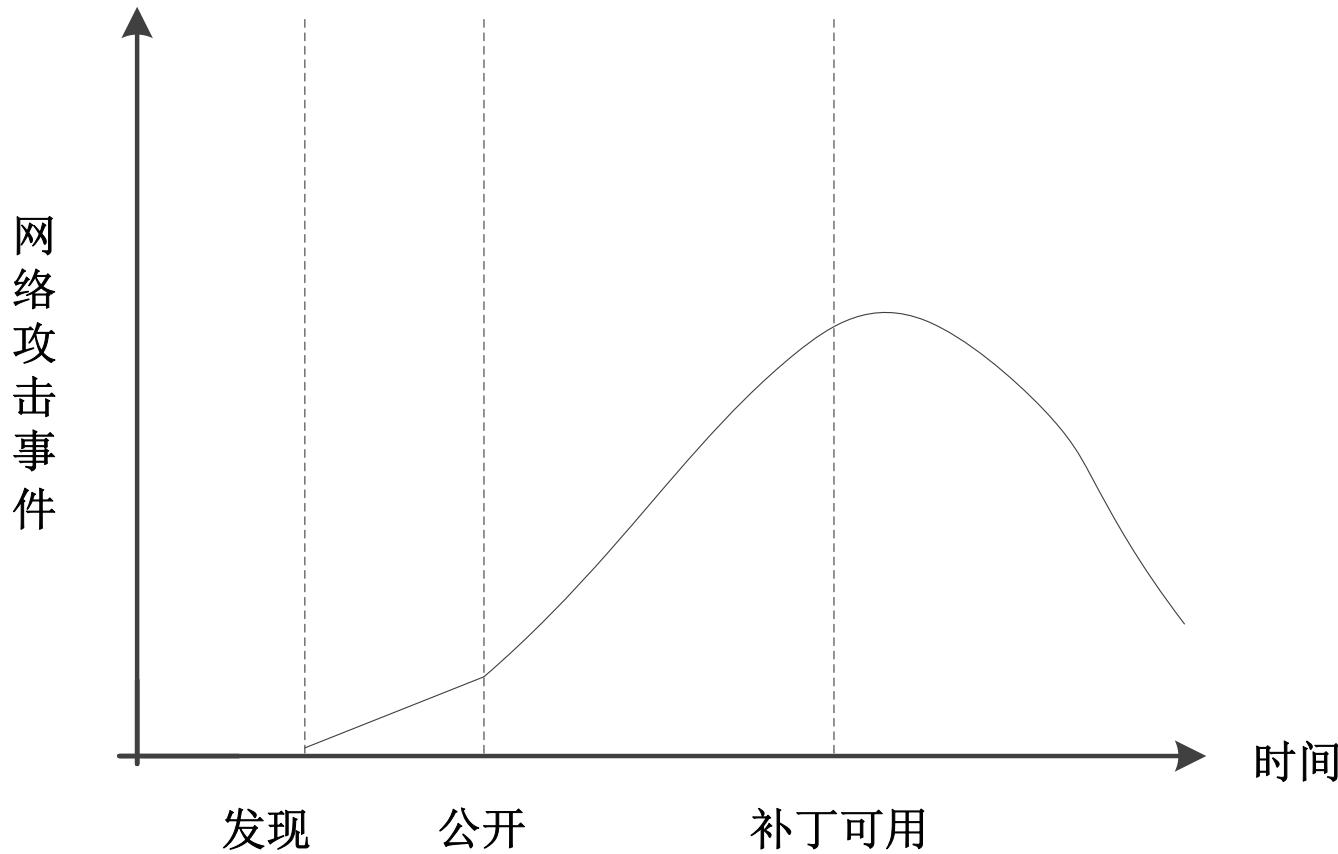
据成绩单显示，孙超然在普渡就读期间的成绩单几乎是清一色全A，而另一名嫌犯、来自日本的留学生白崎成绩也是非常高。当地检方在去年4月对孙、白和另一名印度裔核电子留学生苏嘉伊·夏尔马提出刑事指控，罪名包括入侵电脑、入室盗窃和共谋等罪。



# 安全漏洞生命周期



# 网络攻击事件数目与漏洞生命关系



# 漏洞举例

- DEDECMS是由上海卓卓网络科技有限公司生产的一款网站建站系统软件，在国内政府、高校、企事业单位以及个人用户网站中应用较为广泛。
- 2014年2月25日，该软件被披露存在一个高危漏洞。
- 2月28日，针对该漏洞的攻击利用代码和相关利用工具在互联网上已经被公开传播。
- 漏洞存在于`/plus/recommend.php`页面，由于页面参数未进行严格过滤，存在SQL注入漏洞。

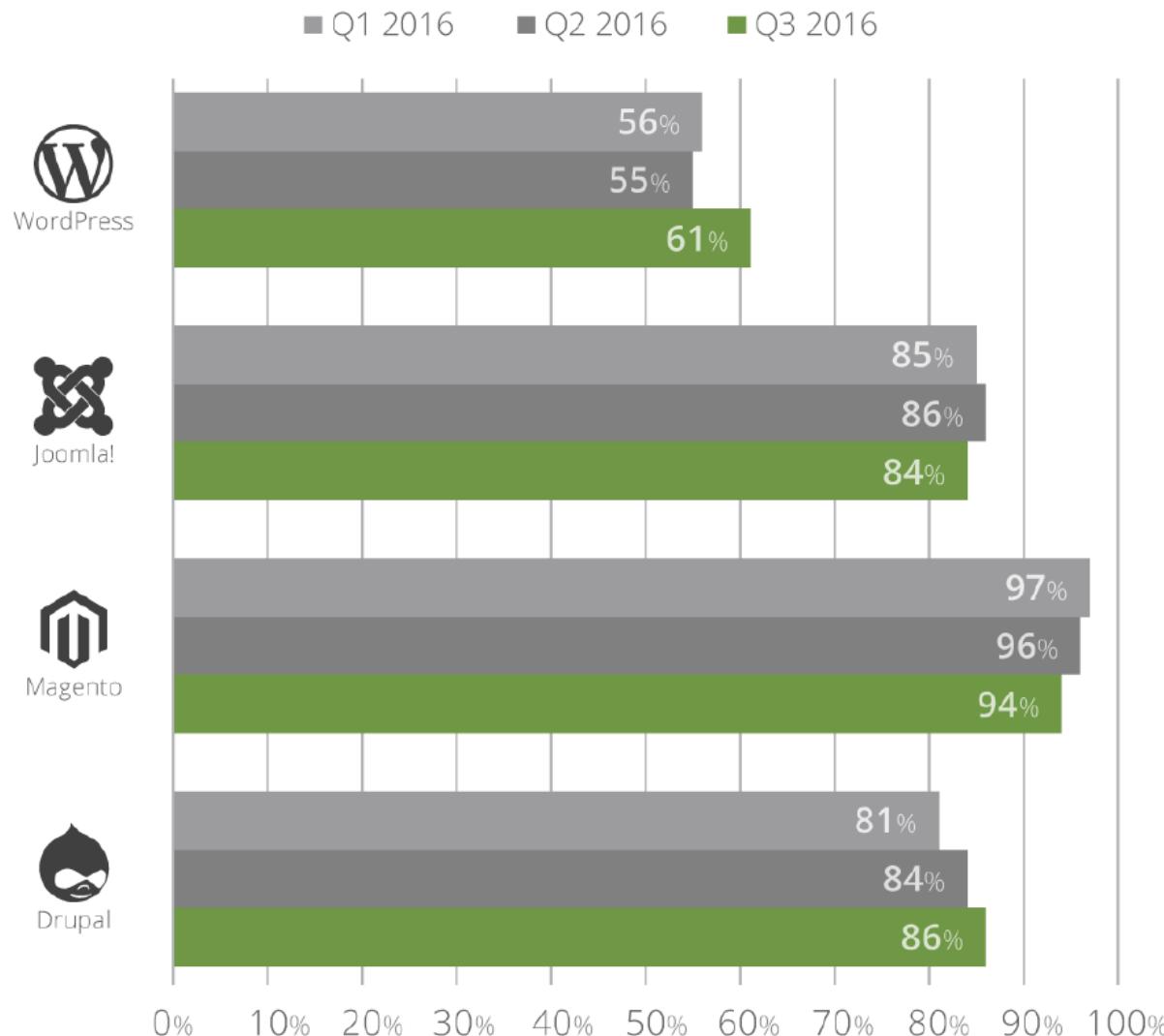


- 3月3日至9日，互联网上有2668个攻击源IP发起漏洞攻击，其中境外攻击源IP占22%（589个），境外攻击源IP中自中国香港地区和美国的较多，分别有163个和155个。
- 上述2668个攻击源IP共尝试扫描了48661个网站IP主机，其中474个网站IP因存在漏洞被攻击成功。在3月8日达到峰值，被攻击成功的网站IP达到286个。



# 很多网站所用的**CMS**版本过期

% of Out-of-Date CMS at Point of Infection Q3 - 2016



- Web服务由什么部分组成？

### 如何识别Web指纹？

插件或扩展

第三方内容：广告统计、mockup

Web前端框架：jQuery/Bootstrap/HTML5框架

Web应用：BBS/CMS/BLOG

Web开发框架：Django/Rails/ThinkPHP

Web服务端语言：PHP/JSP/.NET

Web容器：Apache/IIS/Nginx

存储：数据库存储/内存存储/文件存储

操作系统：Linux/Windows



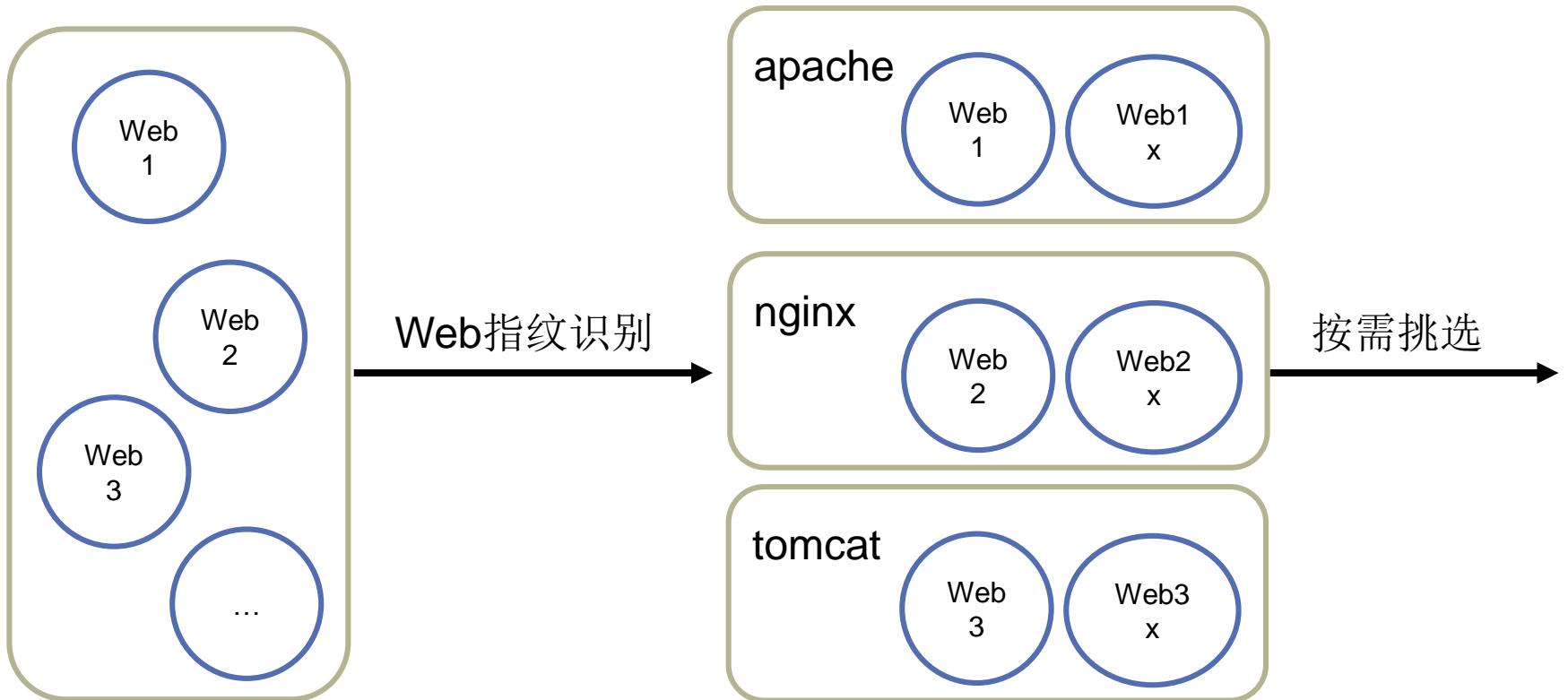
# WEB指纹识别



- 一款用于“回答网站使用什么技术”的工具
- 网站技术包括： CMS系统、 JS库、 Web容器等方面
- 基于插件的形式，最新版本已经包含超过 **1700**个不同的插件，不同的插件用于识别不同的信息
- 同时还能识别出版本号，邮箱地址，账户ID，SQL错误等等的额外信息
- 支持多模式（速度，准确率）运行方式
- 代码托管：<https://github.com/urbanadventurer/WhatWeb>



# WEB指纹识别



# 网络空间探测

shodan

← → ↻ 安全 | <https://www.shodan.io/search?query=wordpress>

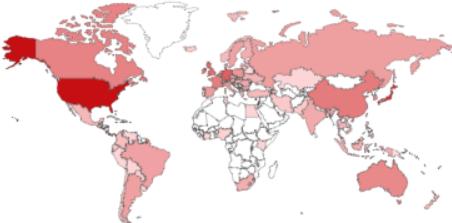
Shodan Developers Book View All...

 SHODAN   Explore Enterprise Access Contact Us

 Exploits  Maps

TOTAL RESULTS **24,296**

TOP COUNTRIES



Country	Results
United States	11,415
Japan	4,319
Germany	1,473
United Kingdom	838
Ireland	667

TOP SERVICES

Service	Results
HTTP	13,827
HTTPS	7,703
SMTP	488
8081	475
9001	429

RELATED TAGS: [wordpress](#) [wps](#)

**モリタ工業株式会社**  
61.126.51.81  
moritakk.co.jp  
**NTT**  
Added on 2017-09-13 05:37:47 GMT  
• Japan  
Technologies:     
[Details](#)

HTTP/1.1 200 OK  
Date: Wed, 13 Sep 2017 05:37:43 GMT  
Server: Apache  
X-Powered-By: PHP/5.3.3  
X-Pingback: http://www.moritakk.co.jp/wordpress/xmlrpc.php  
Transfer-Encoding: chunked  
Content-Type: text/html; charset=UTF-8

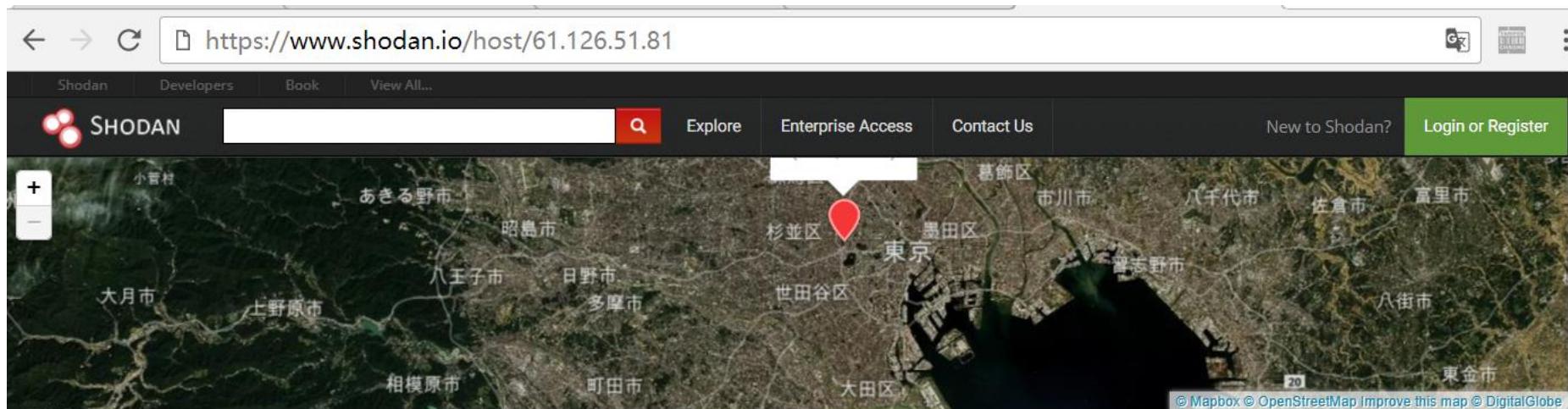
**207.98.157.74**  
dynamic-207-98-157-74.knology.net  
**WideOpenWest**  
Added on 2017-09-13 05:36:31 GMT  
 United States, Columbus  
[Details](#)

HTTP/1.1 200 OK  
Date: Wed, 13 Sep 2017 05:36:30 GMT  
Server: Apache/2.4.7 (Ubuntu)  
X-Powered-By: PHP/5.5.9-1ubuntu4.22  
Vary: Accept-Encoding,Cookie  
Cache-Control: max-age=3, must-revalidate  
WP-Super-Cache: Served supercache file from PHP  
Transfer-Encoding: chunked  
Content-Type: text/html; ...



# 网络空间探测(续)

shodan



61.126.51.81 moritakk.co.jp

Database

Country	Japan
Organization	NTT
ISP	NTT
Last Update	2017-09-13T14:03:12.272494
Hostnames	moritakk.co.jp
ASN	AS4713

## Web Technologies

jQuery

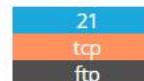
PHP

WordPress

## Ports



## Services



220 FTP Server ready.

530 Login incorrect.

214-The following commands are recognized (\* =>'s unimplemented):

CWD	XCWD	CDUP	XCUP	SMNT*	QUIT	PORT	PASV
EPRT	EPSV	ALLO*	RNFR	RNTO	DELETE	MDTM	RMD
XRMD	MKD	XMKD	PWD	XPWD	SIZE	SYST	HELP
NOOP	FEAT	OPTS	AUTH	CCC*	CONF*	ENC*	MIC*

# WOODYUN事件

- 乌云漏洞平台被认为是是国内最早知名的漏洞报告平台，旨在为厂商和“白帽子”架起一座沟通的桥梁。
- 2016年7月19日下午乌云高管被有关部门约谈，乌云网团队近10人被警方带走（包括乌云CEO方小顿），因何事由暂不明确。

www.wooyun.org

## 乌云及相关服务升级公告

尊敬的各位用户：

为了更好地向大家提供服务，乌云及相关服务将进行升级。我们将在最短的时间内，以最好的姿态回归。

一直以来，乌云致力于让安全性作为用户选择产品的重要考量之一，促进企业更重视安全，让更多人了解安全关注安全，从而营造出更好的安全生态。

不管从前，现在，还是未来，我们都将坚持这么做下去。

与其听信谣言，不如相信乌云。

共勉。

乌云全体成员 敬上  
2016年7月20日



# 中华人民共和国网络安全法

口 第二十七条 任何个人和组织不得从事非法侵入他人网络、干扰他人网络正常功能、窃取网络数据等危害网络安全的活动；不得提供专门用于从事侵入网络、干扰网络正常功能及防护措施、窃取网络数据等危害网络安全活动的程序、工具；明知他人从事危害网络安全的活动的，不得为其提供技术支持、广告推广、支付结算等帮助。



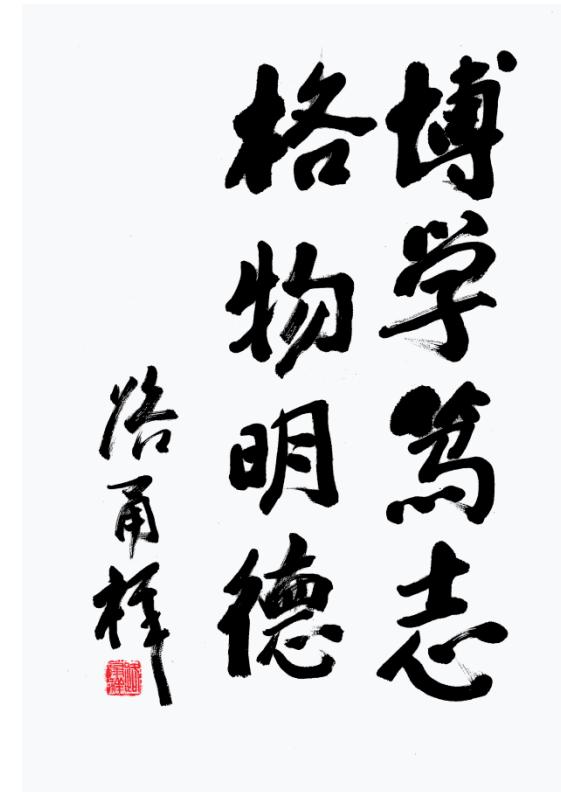
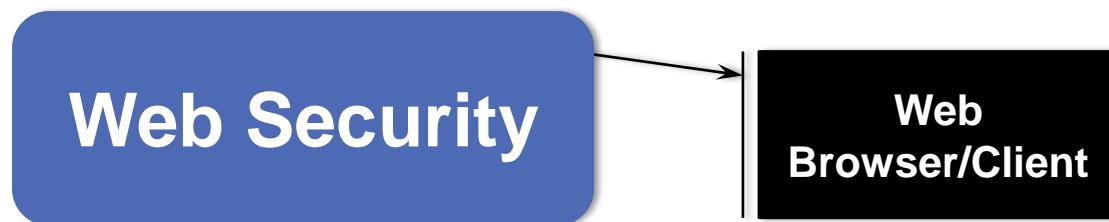
。



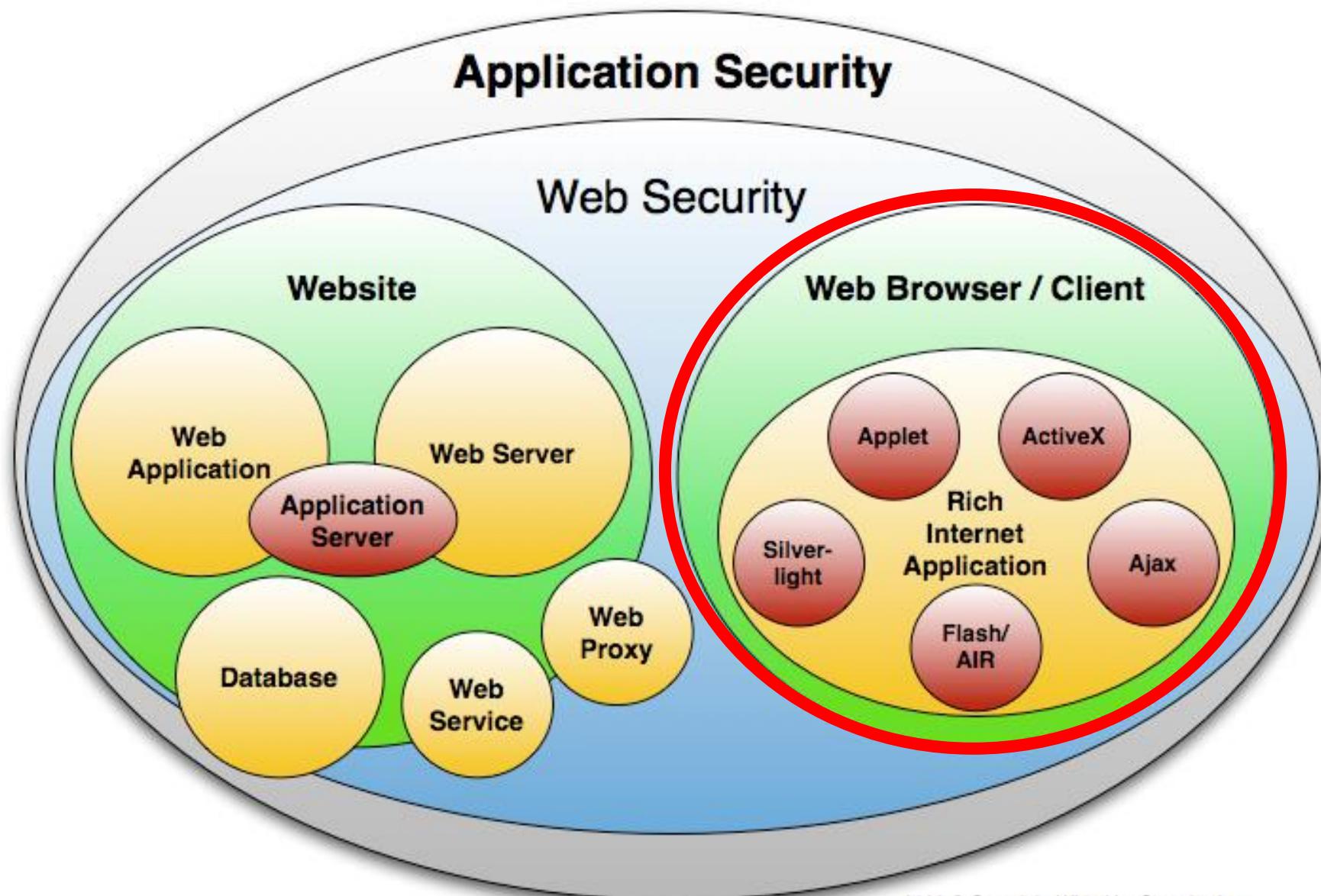
# 本章大纲

□ 网络安全现状

□ Web安全体系结构



# WEB SECURITY



# 极光行动(AURORA)

2010年1月

2010年1月12日，Google称Gmail服务器遭到来自中国的攻击。

搜集Google员工在Facebook、Twitter等社交网站上发布的信息；

利用动态DNS供应商建立托管伪造照片网站的Web服务器，Google员工收到来自信任的人发来的网络链接并且点击，含有shellcode的JavaScript造成IE浏览器溢出，远程下载并运行程序；

通过SSL安全隧道与受害人机器建立连接，持续监听并最终获得该雇员访问Google服务器的帐号密码等信息；

使用该雇员的凭证成功渗透进入Google邮件服务器，进而不断获取特定Gmail账户的邮件内容信息。

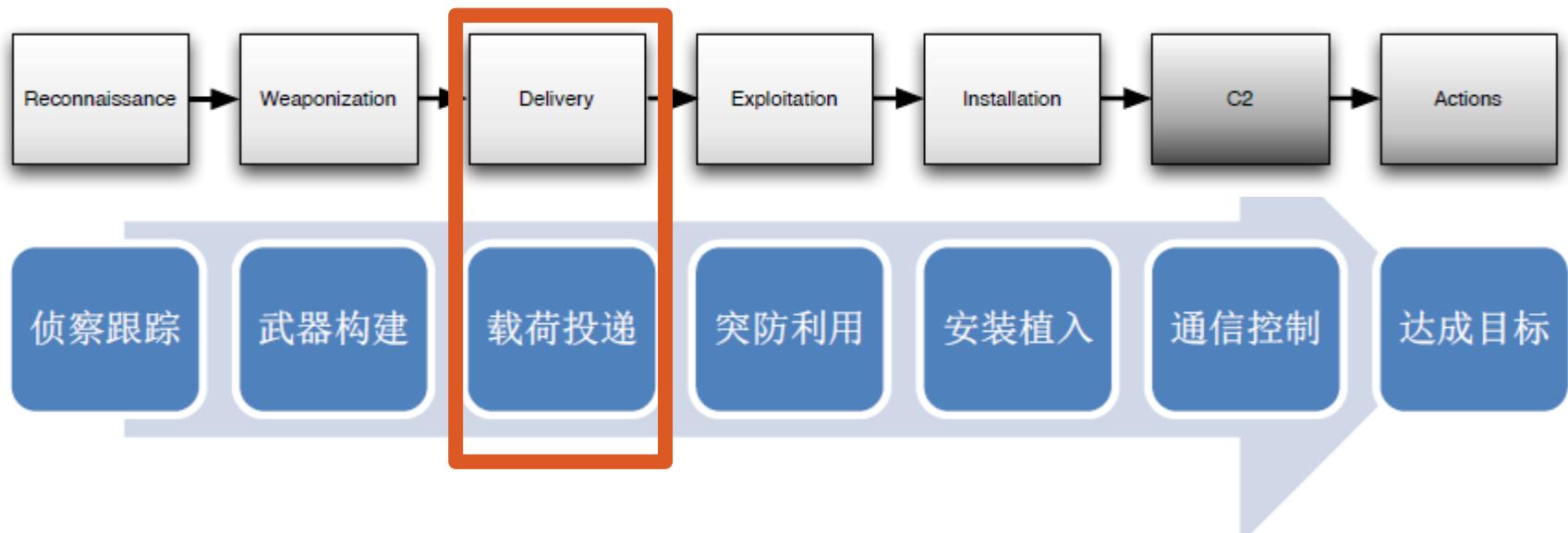


# APT KILL CHAINS

Intelligence-Driven Computer Network Defense  
Informed by Analysis of Adversary Campaigns and  
Intrusion Kill Chains

Eric M. Hutchins\*, Michael J. Cloppert†, Rohan M. Amin, Ph.D.‡

Lockheed Martin Corporation|

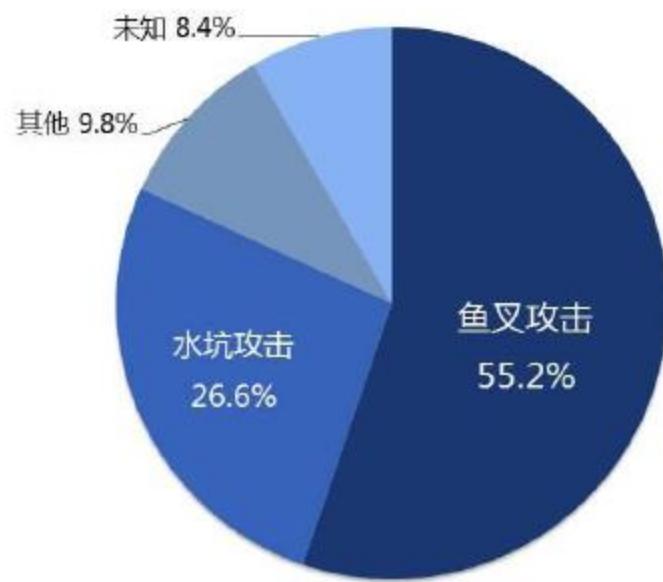


# DELIVERY

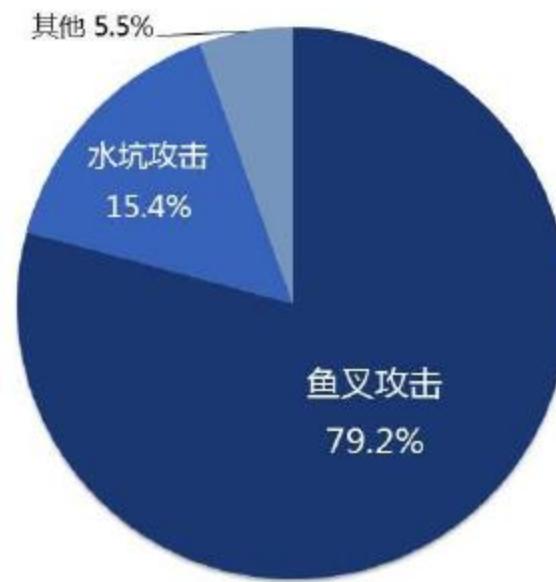
鱼叉式钓鱼邮件攻击和水坑攻击都是 APT 攻击中常用的攻击手法，主要在 APT 的初始攻击环节。

## APT组织相关攻击方式统计

历史累计的APT组织相关攻击方式统计



针对中国的APT组织相关攻击方式统计

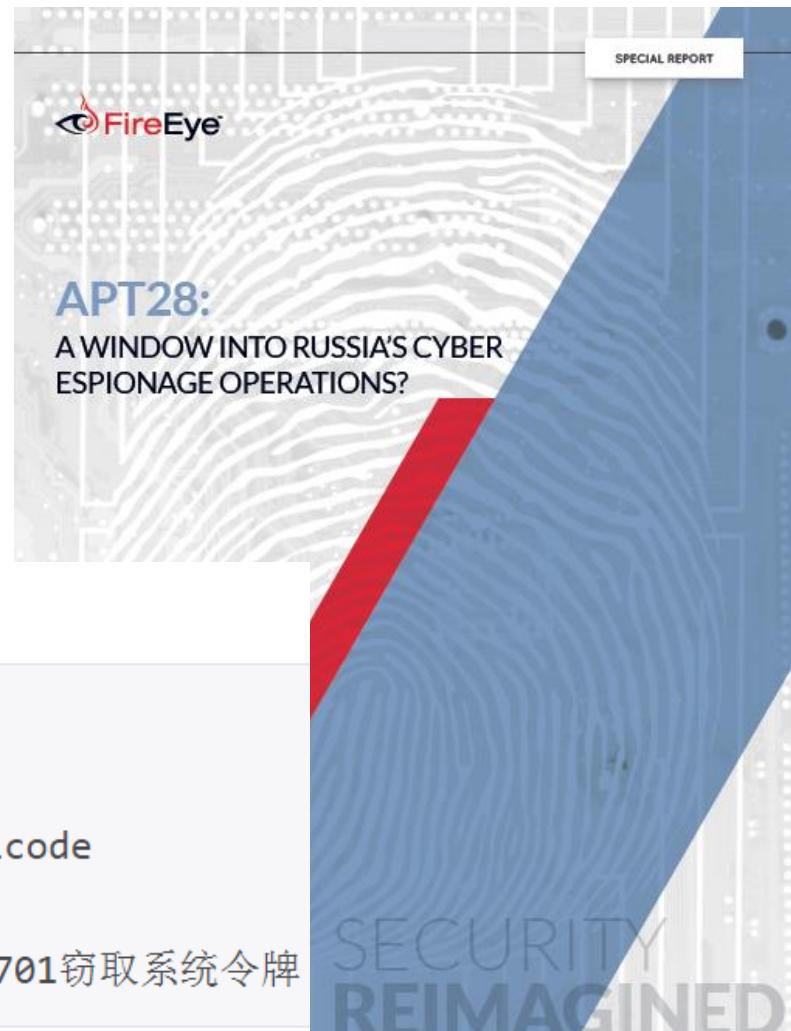


# APT28：专攻军事机构和情报部门

- 该组织发动的攻击活动应始于2007年，而FireEye却在2015年4月13日才首次。
- 此次攻击利用的1个Adobe Flash 0day漏洞(CVE-2015-3043)

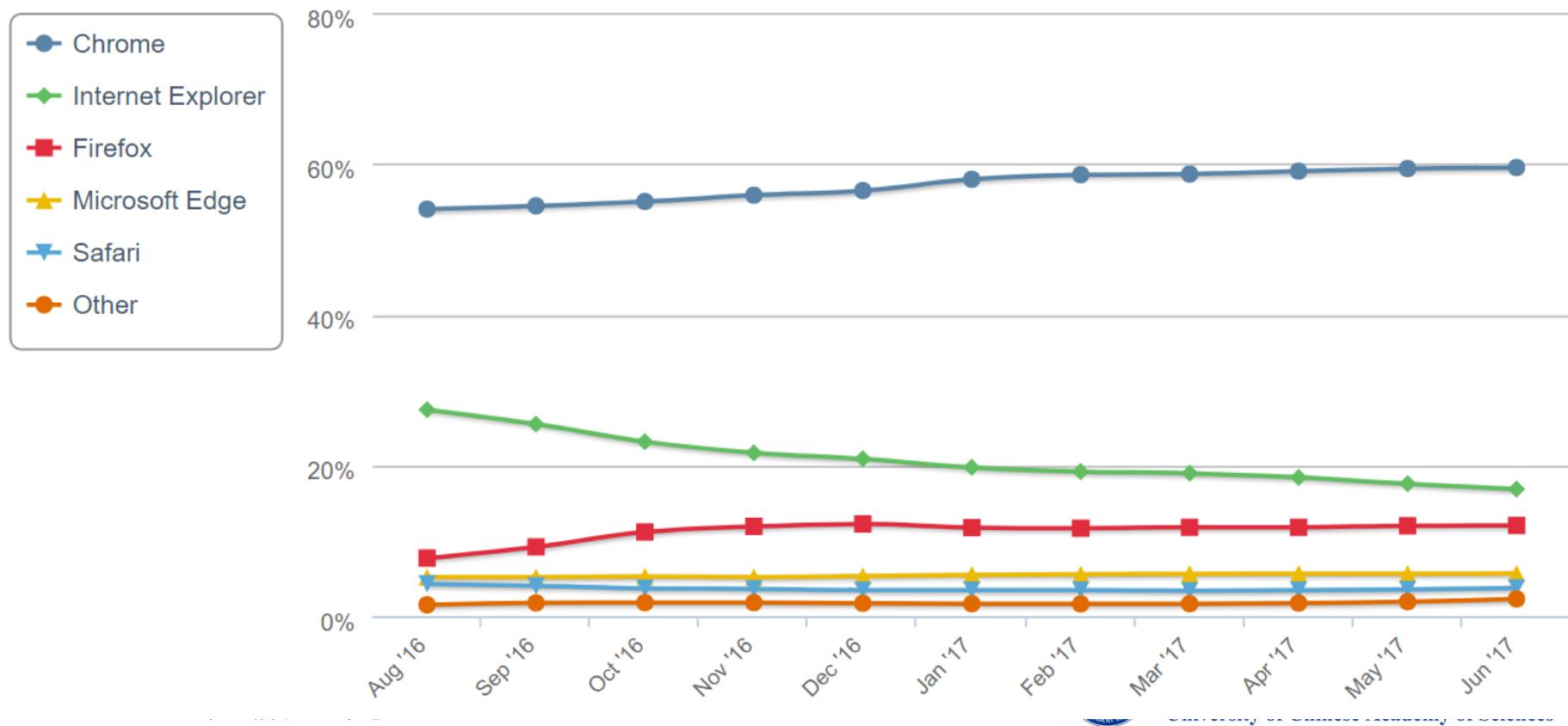
攻击过程如下：

1. 用户访问受攻击者控制的恶意网站
2. HTML/JS启动页面带有漏洞的Flash
3. Flash触发CVE-2015-3043漏洞，执行shellcode
4. Shellcode下载并运行payload
5. Payload利用本地权限提升漏洞CVE-2015-1701窃取系统令牌



# 浏览器市场份额

根据NetMarketShare的报告显示，截至2017年6月，谷歌Chrome市场份额占比59.49%，相比去年同期增长了10.84%。Internet Explorer拥有16.84%的份额，相比去年同期下跌了14.81%，几乎腰斩。



# BROWSER SECURITY

VULNERABILITY REVIEW

2017

Key figures and facts on vulnerabilities from  
a global information security perspective

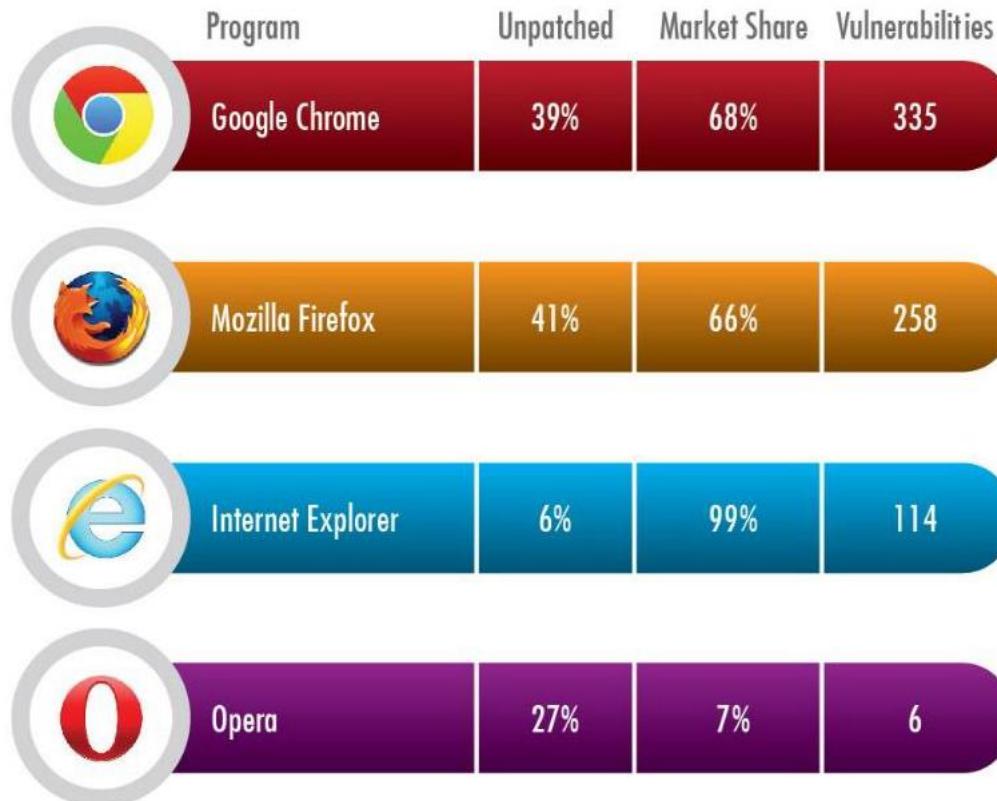


Published March 13, 2017



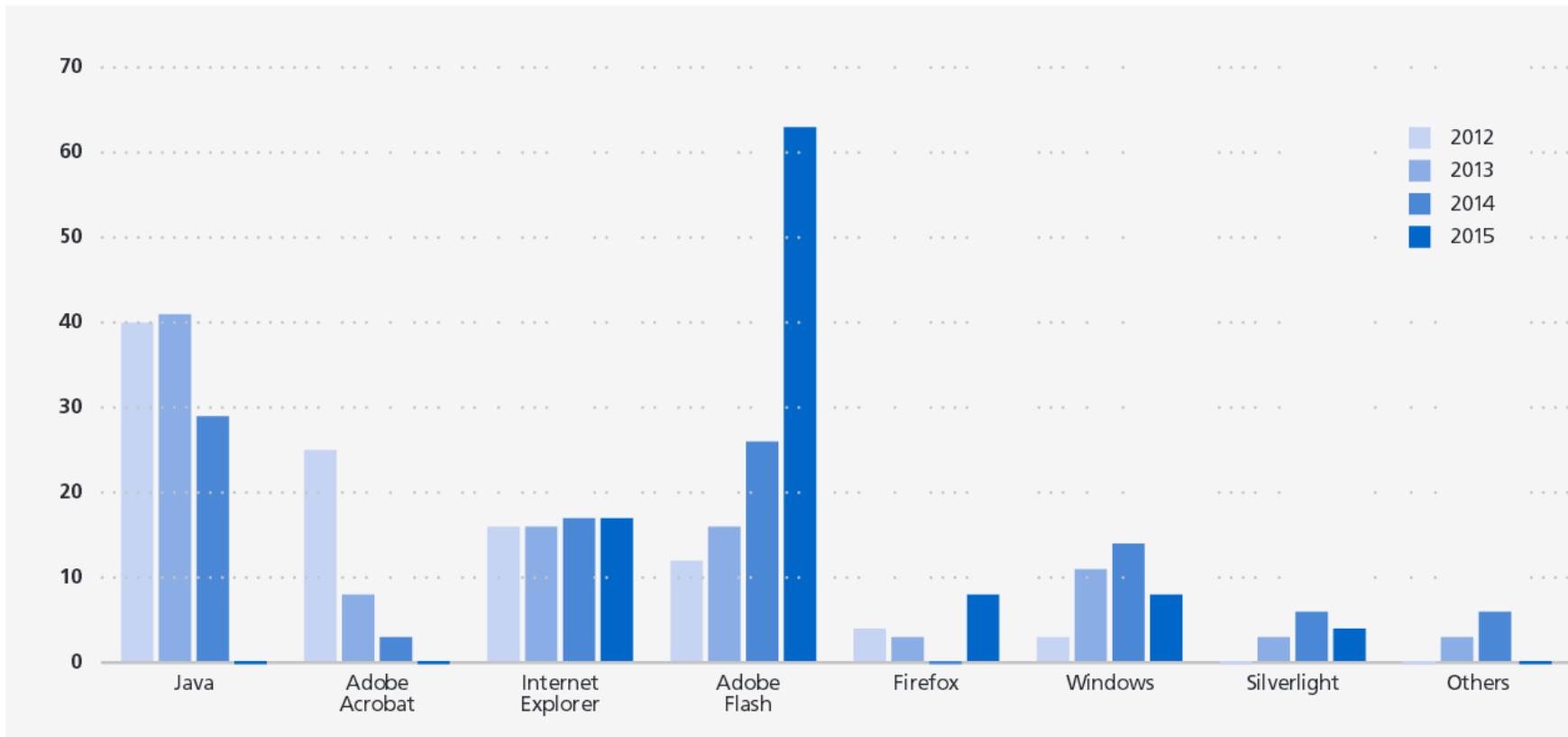
Vulnerabilities indicate the number of new vulnerabilities in the last 12 months.

Market share is percentage of Personal Software Inspector users  
with the product installed on their PC.



# 2015年十大最危险漏洞

- 2012-2014年，Java的漏洞“利用率”一直都是最高的，2015年则是Flash第一次“夺魁”，Java则几乎销声匿迹，位列第二第三的分别是IE浏览器、Windows操作系统。



# HACKING TEAM

- 2015年，意大利专门从事hacking活动的Hacking Team被黑，400G资料在网上泄露传播。
- 本次泄漏包括了Adobe Flash Player 0day（影响IE、Chrome等）。

## Index of /

Name	Last Modified	Size	Type
Parent Directory/	-	-	Directory

Adobe Flash 的安全性一直饱受争议，被誉为“黑产军团的军火库”。APT28 和 Pawn Strom 都利用了 Adobe Flash 的 0day 漏洞进行 APT 攻击，2015 年全年上报的 Flash 漏洞更是多达 300 余条。Hacking -Team 的数据泄露事件，将 Flash 漏洞的实际危害性和影响力推到当年顶点，暴露出的三个漏洞几乎能够影响所有平台、所有版本的 Flash。其中被发现的第二个漏洞（CVE-2015-5122）甚至被黑客团队戏称为“过去四年里最漂亮的 Flash 漏洞”。

Exploit_Delivery_Network_android.tar.gz	2015-Jul-06 13:31:32	797.1M	application/gzip
Exploit_Delivery_Network_windows.tar.gz	2015-Jul-06 13:43:50	716.5M	application/gzip
support.hackingteam.com.tar.gz	2015-Jul-06 21:22:48	15.1G	application/gzip

# PWN2OWN

Pwn2Own是全球黑客顶级赛事，以黑客“世界杯”著称，由美国国防部安全服务商、惠普旗下TippingPoint的ZDI项目组主办，微软、苹果、谷歌、Adobe、Intel等领导厂商提供赞助，旨在支持和鼓励帮助他们发现操作系统、浏览器、游戏引擎等软件平台安全漏洞的优秀人才。

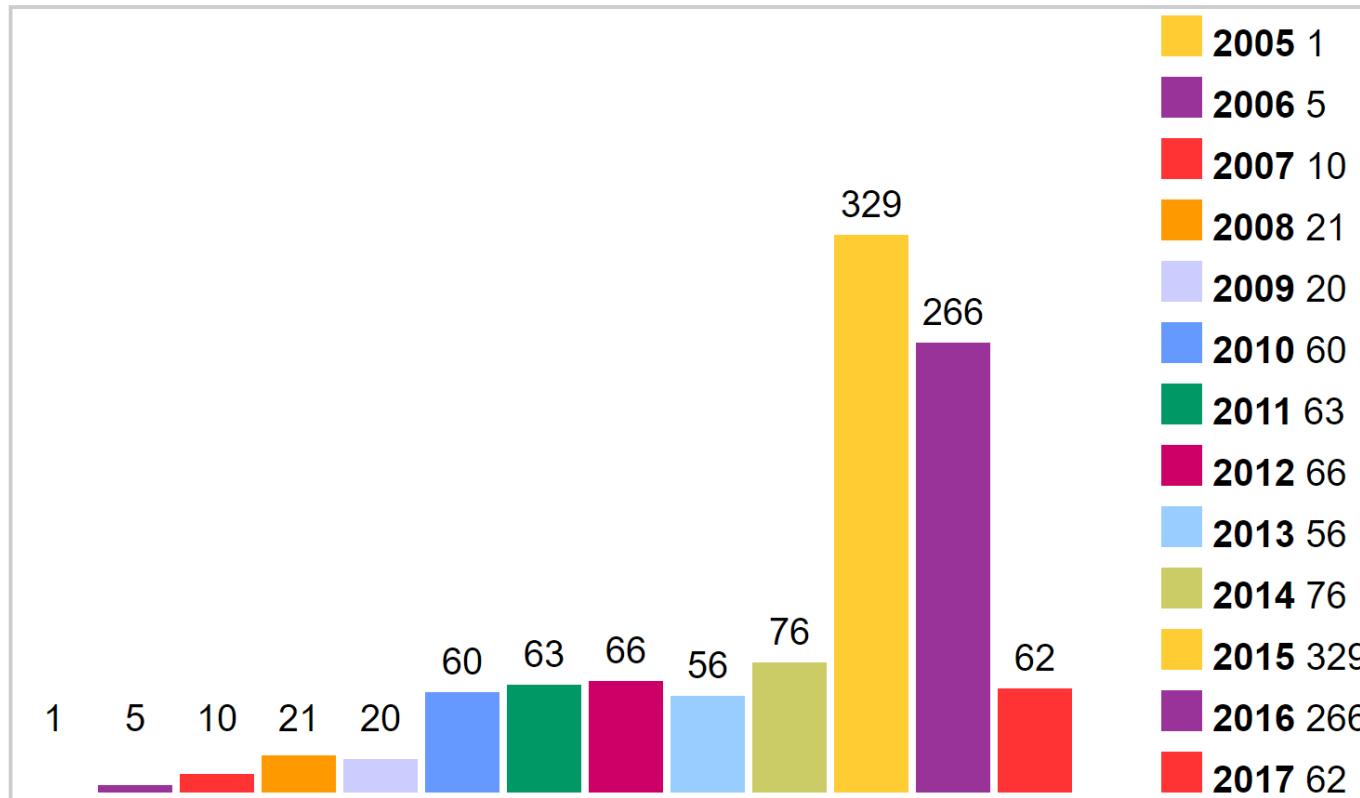
表2 我国网络安全研究团队/个人成功参加国际性安全破解大赛的历史成绩

年份	安全破解赛	队伍/个人	比赛项目
2016	Pwn2Own	腾讯安全Sniper战队 (KEEN和电脑管家)	Adobe Flash
2016	Pwn2Own	腾讯安全Sniper战队 (KEEN和电脑管家)	苹果Safari浏览器
2016	Pwn2Own	腾讯安全Sniper战队 (KEEN和电脑管家)	微软Edge浏览器
2016	Pwn2Own	奇虎360-Vulcan	Adobe Flash
2016	Pwn2Own	奇虎360-Vulcan	Google Chrome 浏览器
2016	Pwn2Own	腾讯安全Shield战队 (电脑管家和KEEN)	苹果Safari浏览器



# ADOBEBE FLASH 漏洞

Vulnerabilities By Year



Adobe决定在2020年停止支持Flash

# 浏览器漏洞攻击包

## browsersploit

BrowserExploit is an advanced browser exploit pack for doing internal and external pentesting, helping gaining access to internal computers.

I started this project years ago, when still exploiting IE 6, 7 and 8. The exploits in kit are old so it keep scripts kiddies from running it in the wild and achieve malicious task.

BrowserSploit use a lot of techniques to bypass anti-virus and is full of featured.

- Javascript obfuscation (XOR, JS Iframe Head, Cookie Encrypted, Split Encrypted Iframe, Base64 random space).
- Advanced exploitation techniques.
- Artificial Intelligence based on traffic learning.
- Multi-Users ready platform
- Filter Antivirus connections
- Evade AV domain filters
- Reverse Honeypot features to trick non legitimate users and sec users
- Bypass Windows DEP / ASLR / UAC
- Advanced polymorphic shellcoding

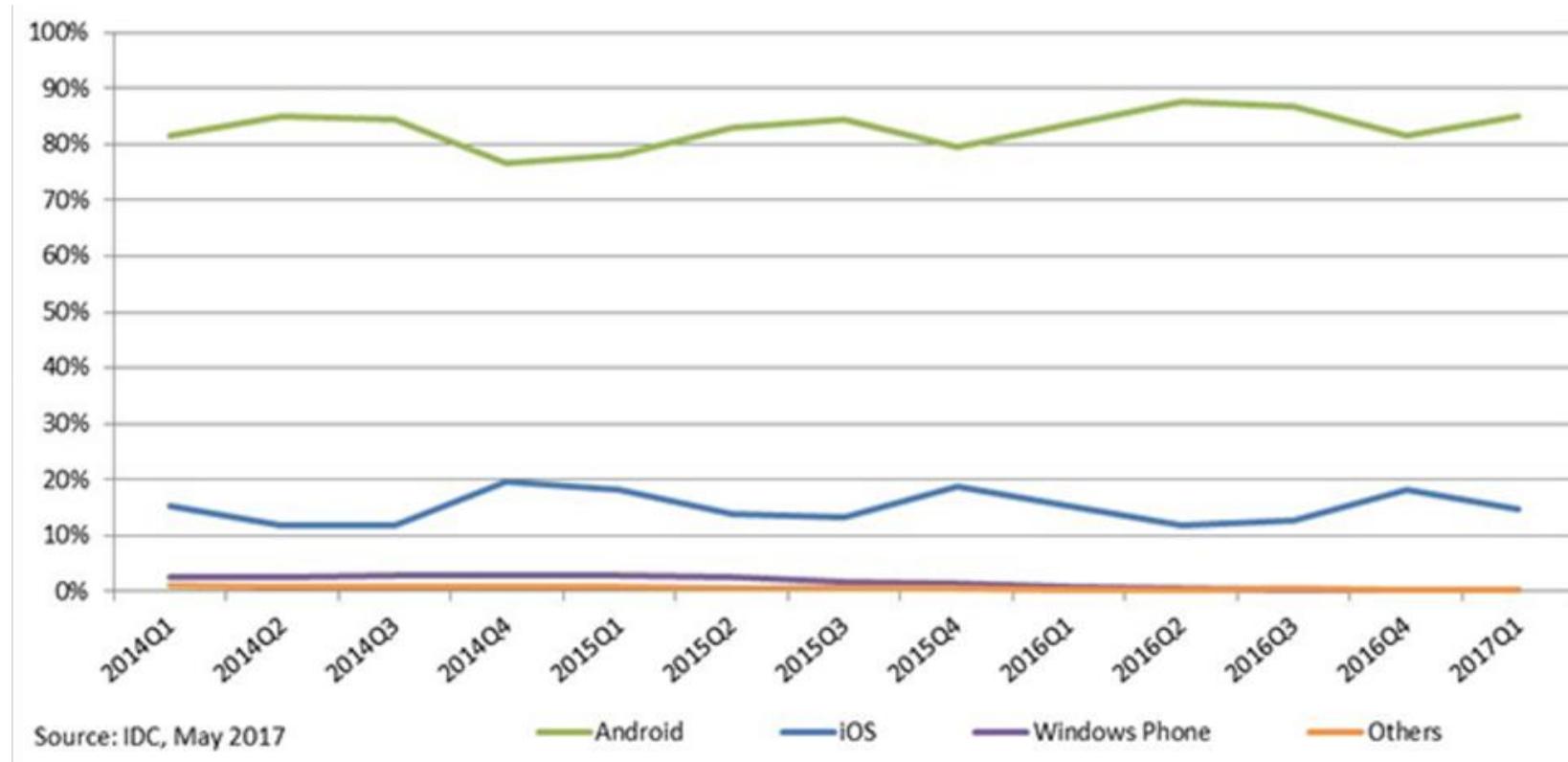
What it mean for the non-technical people: If you surf the web on your browser and you visit a page infected by an browser exploit pack, then you will likely be infected by malicious software without even notify it.



# 智能终端



## □ IDC: Android Captures 85% Of Smartphone Market In Q1 2017



<https://www.idc.com/promo/smartphone-market-share/os>

## □ IDC: Android Captures 85% Of Smartphone Market In Q1 2017

Period	Android	iOS	Windows Phone	Others
2016Q1	83.4%	15.4%	0.8%	0.4%
2016Q2	87.6%	11.7%	0.4%	0.3%
2016Q3	86.8%	12.5%	0.3%	0.4%
2016Q4	81.4%	18.2%	0.2%	0.2%
2017Q1	85.0%	14.7%	0.1%	0.1%

Source: IDC, May 2017

<https://www.idc.com/promo/smartphone-market-share/os>



## 使用了过低版本的chromium定制内核的APP会存在未知的远程代码执行漏洞，如近日“BadKernel”漏洞

近日，360手机卫士阿尔法团队再次发现Chrome V8引擎“BadKernel”漏洞。该漏洞存在于V8引擎的历史版本中，远程攻击者可利用该漏洞对使用受影响引擎的产品进行远程攻击。

通过此漏洞攻击者可实现微信远程代码执行，获取微信的完全控制权，危及用户朋友圈、好友信息、聊天记录甚至是微信钱包，可使上亿微信用户受到影响，危害巨大。由于腾讯浏览服务提供的X5 SDK中的X5内核集成了Chrome V8引擎，该引擎受上述漏洞影响。根据腾讯浏览服务介绍，使用X5 SDK的微信、手机QQ、QQ空间、京东、58同城、搜狐视频、新浪新闻等Android手机APP均可能受该漏洞影响。利用该漏洞在微信Android APP上实现反弹shell的视频如下：

<http://weibo.com/p/2304445bee6e775e81ad8b0486eaa519ea223b>

该问题影响的版本是使用V8引擎3.20至4.2版本的厂商。影响Android 4.4.4至5.1版本系统，以及使用相关组件和定制组件的APP。

# NFC

- NFC(Near Field Communication)技术是一种近距离的双向高频无线通信技术，能够在移动终端、智能标签(Tag)等设备间进行“**触碰**”或“**靠近**”进行数据传输(包括文字、音乐、照片、视频等)、数据访问、电子支付等操作。
- NFC技术是从射频识别技术、感应识别和互联技术演变而来，由飞利浦、诺基亚和索尼共同研制开发，运行在13.56MHz频段，有效传输距离为0~20cm(主动通信20cm，被动通信10cm)，传输速率为106k/s、212k/s或424k/s，与Mifare和Felica RFID标准相兼容。



9

点对点模式



读卡器模式



卡模拟模式

学  
University of Chinese Academy of Sciences

# NFC:卡模拟模式

iPhone 6

Explore ■■■

Buy Now



Your wallet.  
Without the wallet.

We completely rethought how you pay to make shopping easy, secure, and private. Apple Pay combines the convenience and security of Touch ID and Passbook with NFC technology. So you can use iPhone 6 to pay in stores and within apps with a single touch.

[Learn more about Apple Pay >](#)

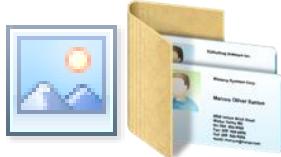
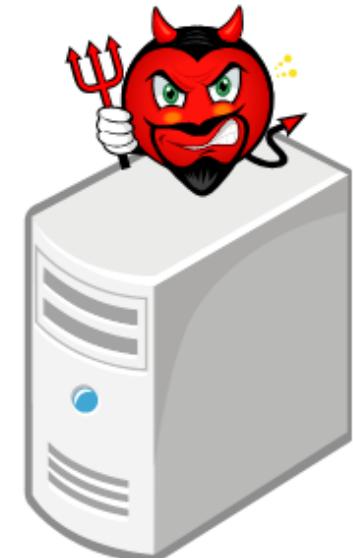
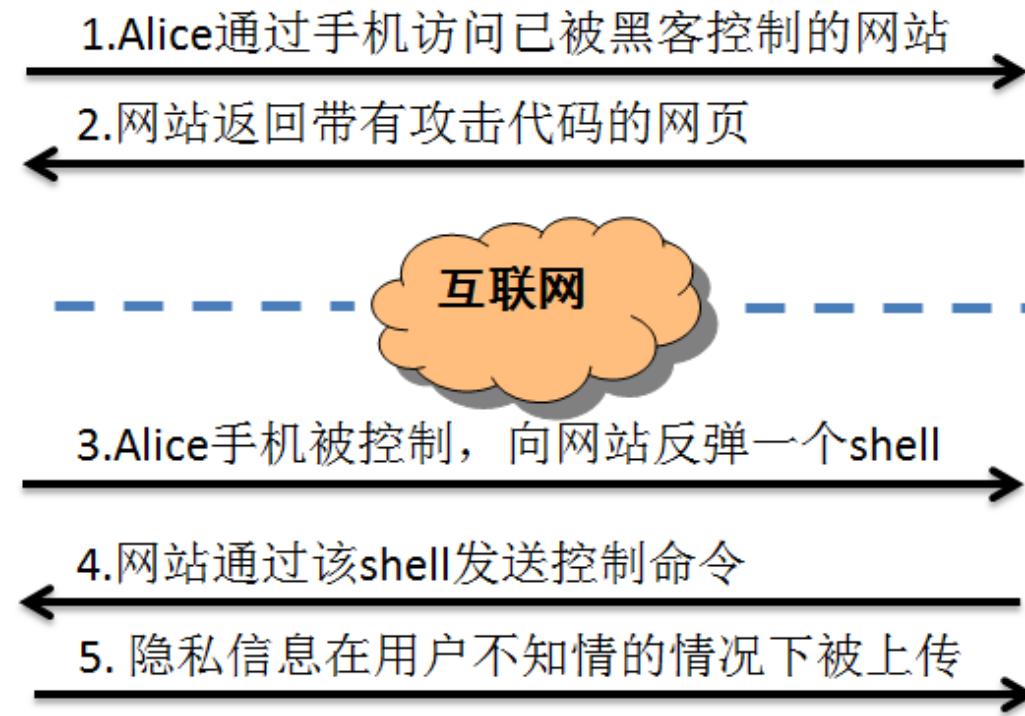
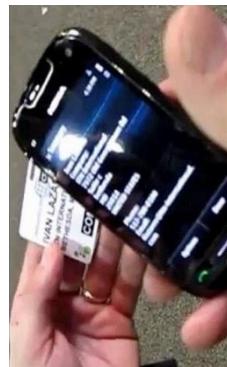


# NFC:读卡器模式

- 它可以作为非接触读卡器使用，能从各种电子标签上读取相关信息。就像是我们现在所使用的微信扫描一样，只是这种技术更加完善，不一定要是二维码，而可以使各种电子标签。



# 发生了什么？





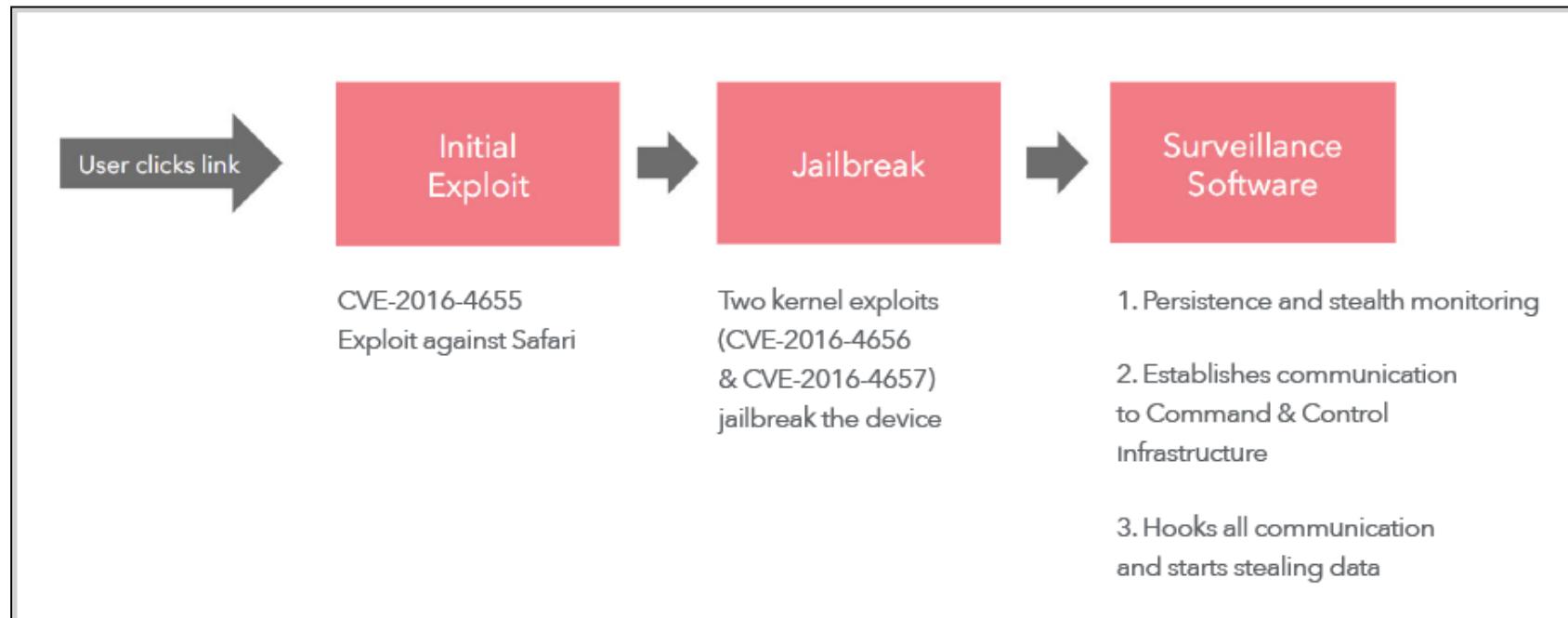
# PEGASUS

- iOS 9.3.5于2016-08-26紧急上线，苹果更新日志中有提到修复了“重要安全问题”。涉及的iOS安全问题可能是“前所未有”的。
- Pegasus影响的iOS版本，从最近的iOS 9.3.4一直到较早的iOS 7
- 苹果所指的重要安全问题乃是说3个0-day漏洞，这3个漏洞足以让攻击者对全球范围内的iPhone进行监听。



# PEGASUS

- 整个攻击过程首先是通过短信、引诱受害者访问某恶意站点，感染用户级别权限的恶意程序，随后可提权获取内核级别权限。
- 对这次漏洞的利用而言，只需要点击一个网址，就能达到越狱的效果，真正做到了“一键越狱”。



1、攻击者首先通过 SMS 短信把一个链接发送给目标任务，当目标任务点击链接之后，会访问攻击者的一个网站。

2、攻击者的网站上会放置一个针对 Mobile Safari 的攻击程序，这个程序中，包含了 MobileSafariJavascript 引擎的一个0day漏洞。 CVE-2016-4657

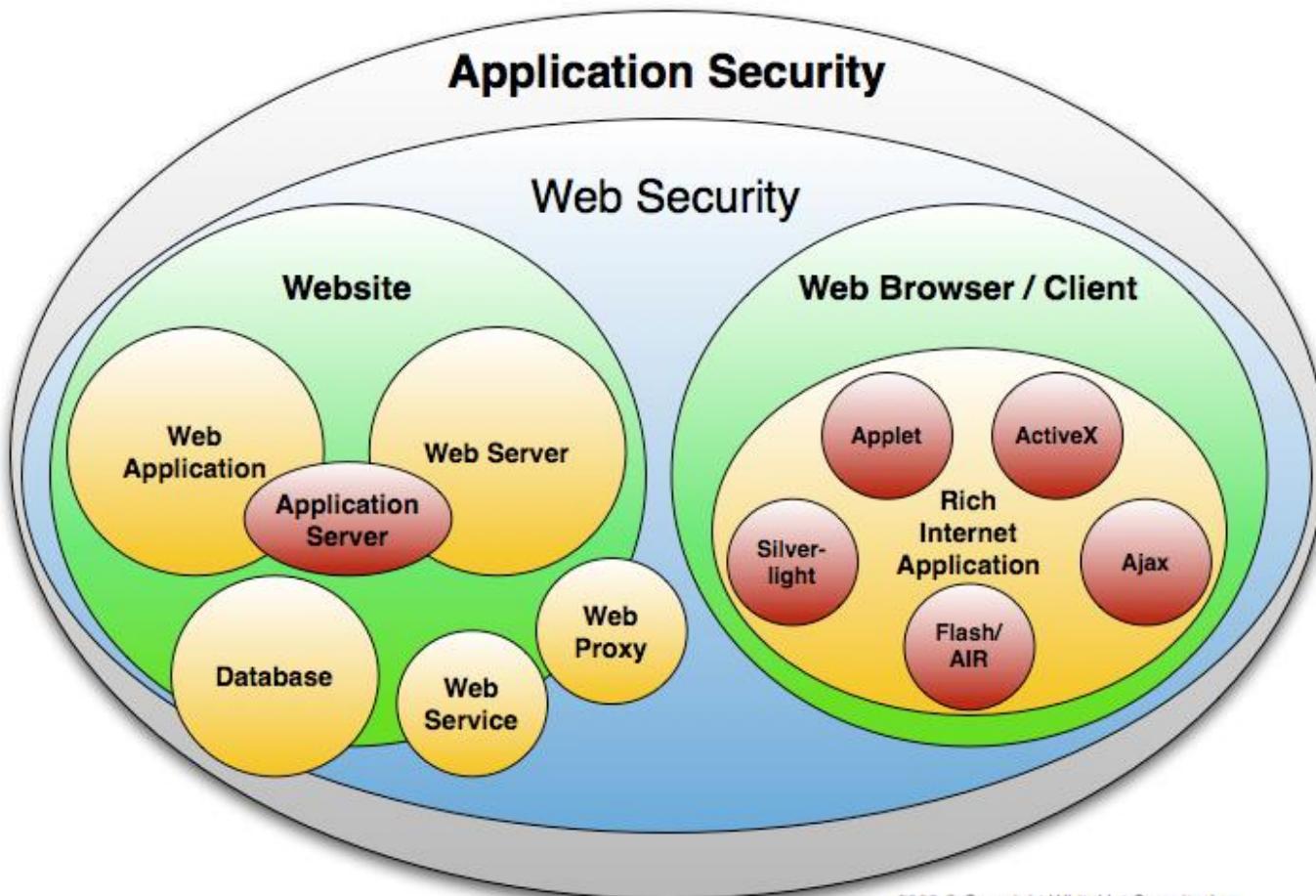
3、攻击程序被执行之后，攻击者会通过浏览器获得手机的执行权限。此时攻击者的权限还只是被囚禁在沙盒之内。

4、接下来，攻击者通过两个内核漏洞（一个内核信息泄露漏洞+一个内核代码执行漏洞）获得内核执行权限。

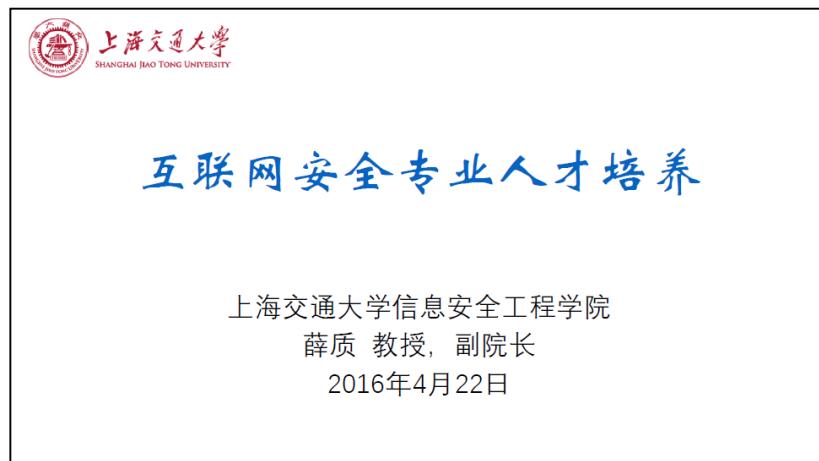
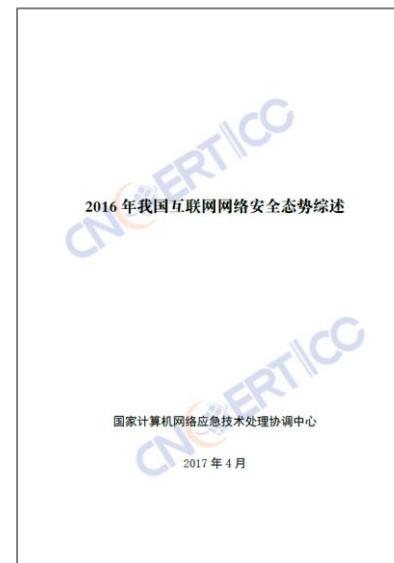
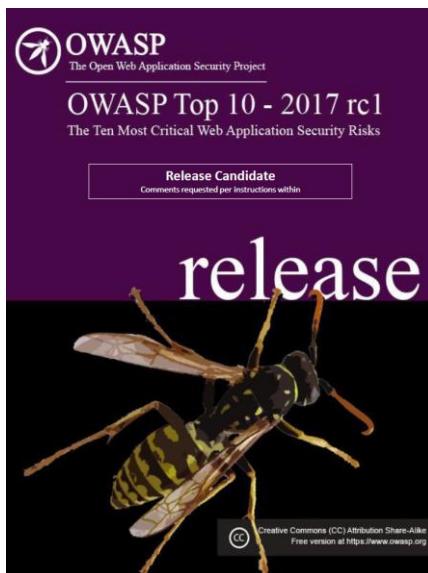
5、获得内核执行权限后，攻击者就完成了手机越狱。这时他会关闭一些iOS的安全保护机制，比如开启rootfs的读写，关闭代码签名等等。

6、完成攻击之后，入侵者就成为了手机的“主人”，可以实现对手机通信、流量的全面监听。

# 小结



# 参考文献



# 后续课程内容

- 第一部分：基础知识
- 介绍Web安全定义与内涵，国内外现状与趋势、近年来重大网络安全事件等，以及本课程可参考的书籍和网络资源；介绍本课程所需掌握的基础知识，包括HTTP/HTTPS协议、Web前后端编程语言、浏览器安全特性等。
- 1.1 绪论
- 1.2 Web的简明历史
- 1.3 同源策略
- 1.4 HTTP与Cookie





[2017秋]Web Security

扫一扫二维码，加入该群。

# 谢谢大家

刘奇旭

liuqixu@iie.ac.cn

中科院信工所 第六研究室



中国科学院大学  
University of Chinese Academy of Sciences