网络安全概要

段海新

2024/09/12

概要

- 网络安全学科的特点
- 风险分析及实例
  - 资产（Assets）
- 漏洞（Vulnerabilities）
- 威胁（Threats）

网络安全：网络中人和人的攻防对抗

- 安全可靠
  Safety, Reliability

- Security：存在敌手的环境(Adversary Context)
  - 在有敌人窃听、干扰的环境中传输敏感数据

信息安全的三个基本概念

Confidentiality

- 保密性或机密性：
  - 保证信息、资源只能由授权的用户访问
- 实现机制：
  - 加密：使敌手既使得到数据，但读不懂信息
  - 访问控制，让敌手无法得到数据

Integrity

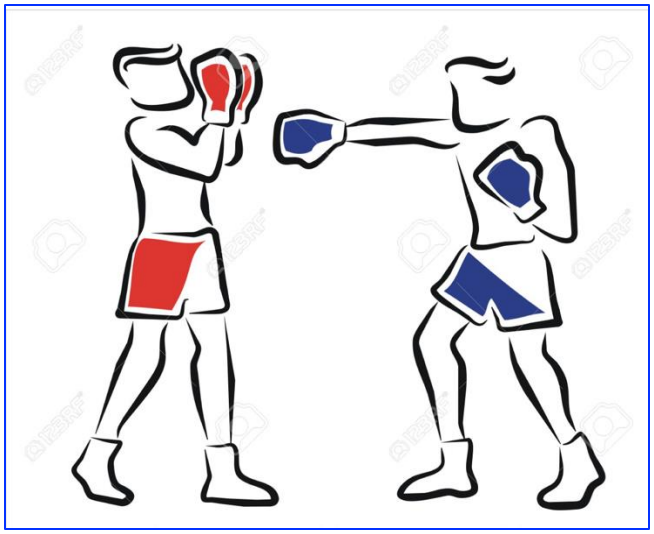
- 完整性：
  - 确保保护的对象是没有被未授权的用户篡改过。
- 实现机制：
  - 数字签名
  - 访问控制

Availability

- 可用性：
  - 系统或资源对授权的用户是持续访问的，
- 实现机制
  - 设计和实现上避免单一故障点
  - 资源的冗余备份

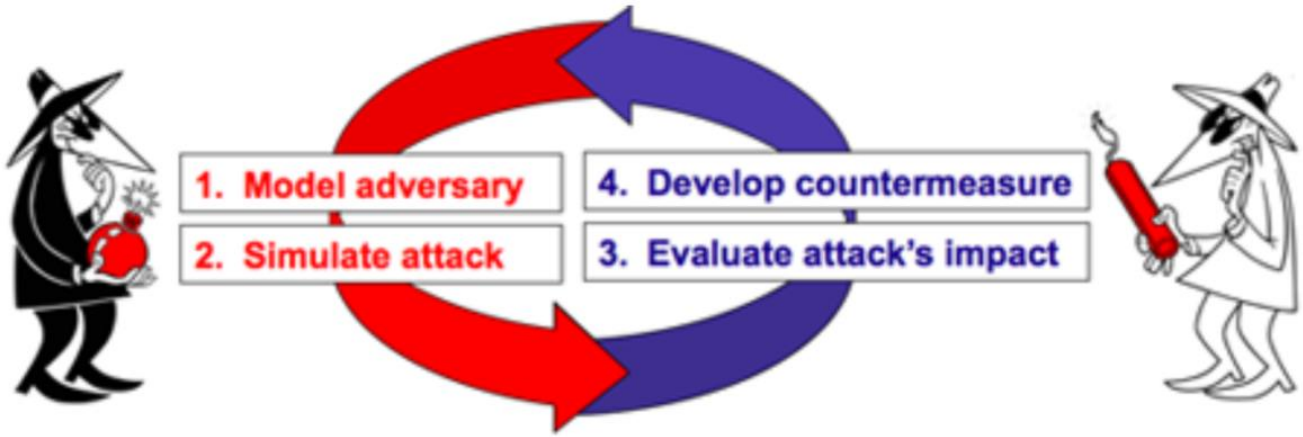
必须有一个敌手(Adversary)

- 网络空间中人和人的冲突与对抗
  - 个人、网络犯罪；
  - 商业上的竞争对手
  - 国家和国家之间



持续的军备竞赛（Arm Race）

- 你的攻击/防范措施，对方如何应对？
- 然后你再怎么做？



Arm Race 实例

- Virus ➔ Analysis in VM=> VM identification
- Virus -> Signature detect-> Pack-> Unpack
- Intrusion=> IDS => evasion
  - Detection(snort):

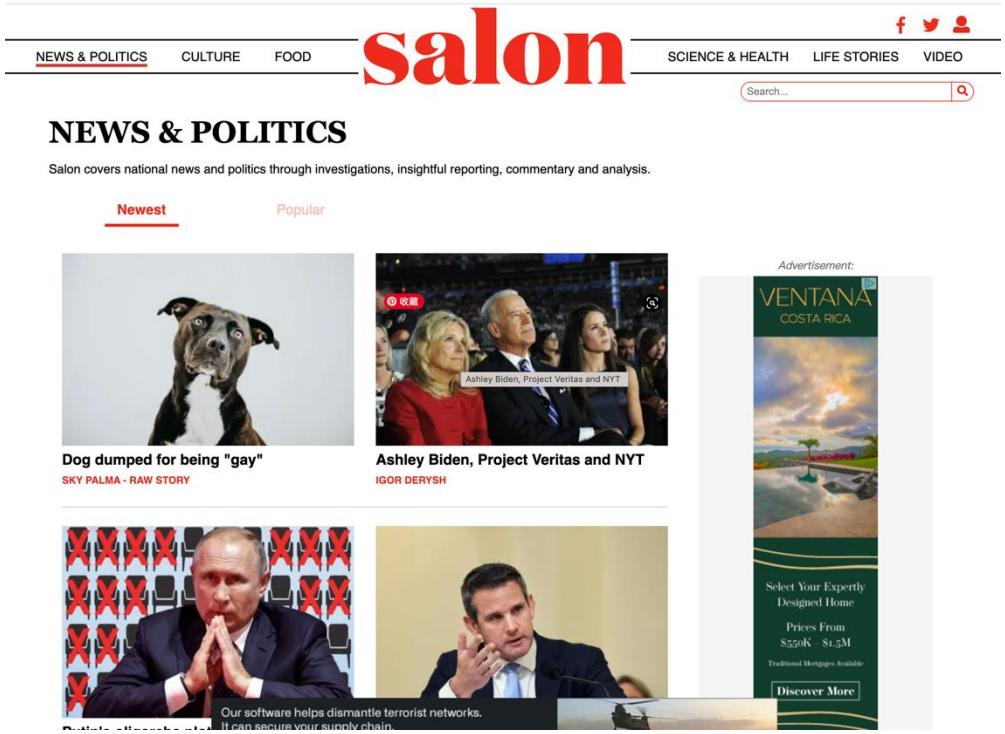
```
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS 80 (msg:"WEB-MISC
/etc/passwd";flags: A+; content:"/etc/passwd"; nocase;
classtype:attempted-recon; sid:1122; rev:1;)
```

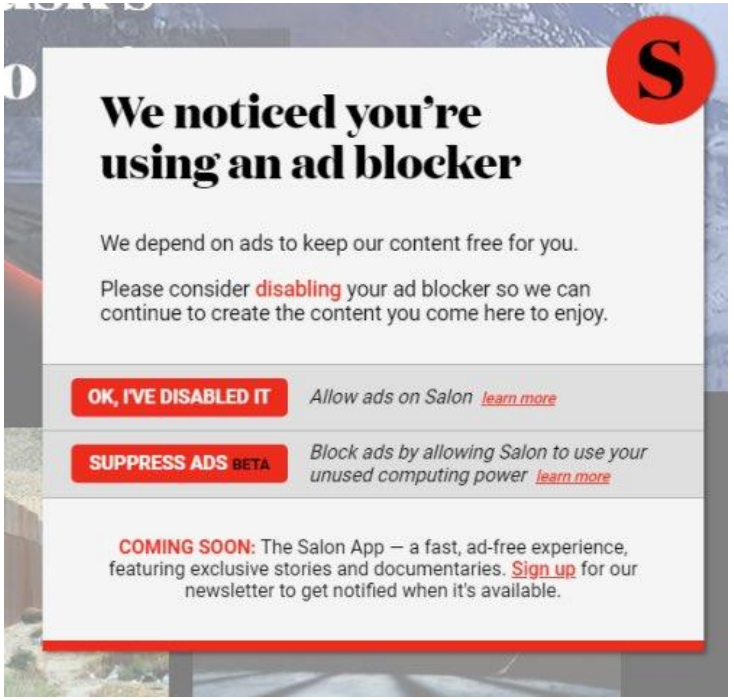
  - Evasion:

```
GET /etc/init.d/../passwd
```

AD => AD-Block =>Anti-ADB =>Anti-Anti-ADB

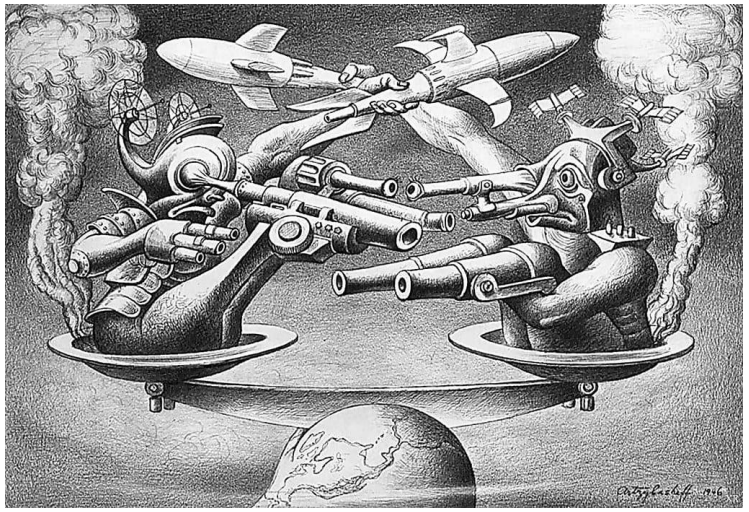
- 实例：某网站对安装AD Blocker的用户弹窗





看我的广告，还是让我用你的计算机挖矿？

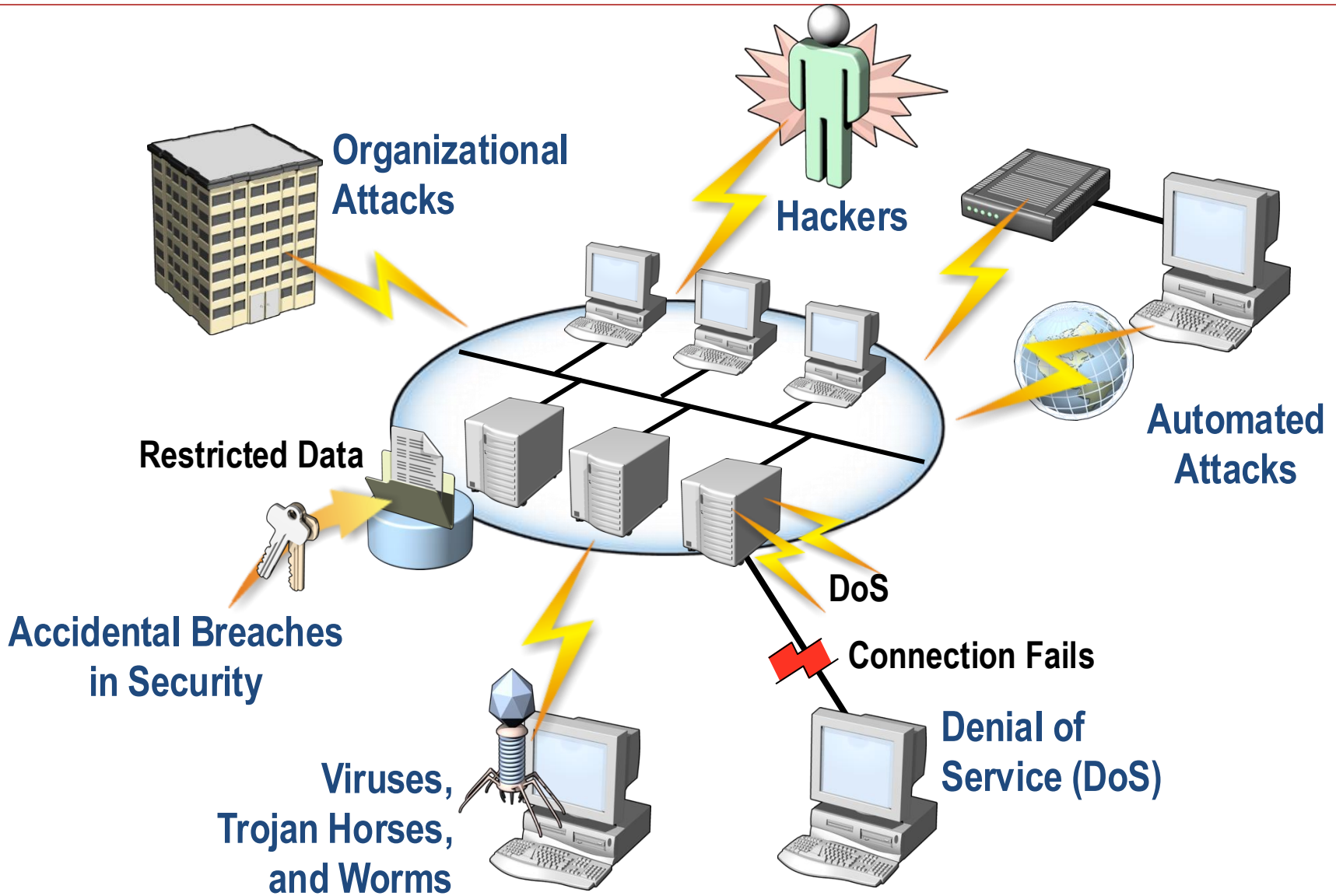
Arm Race, 赢家是谁呢？



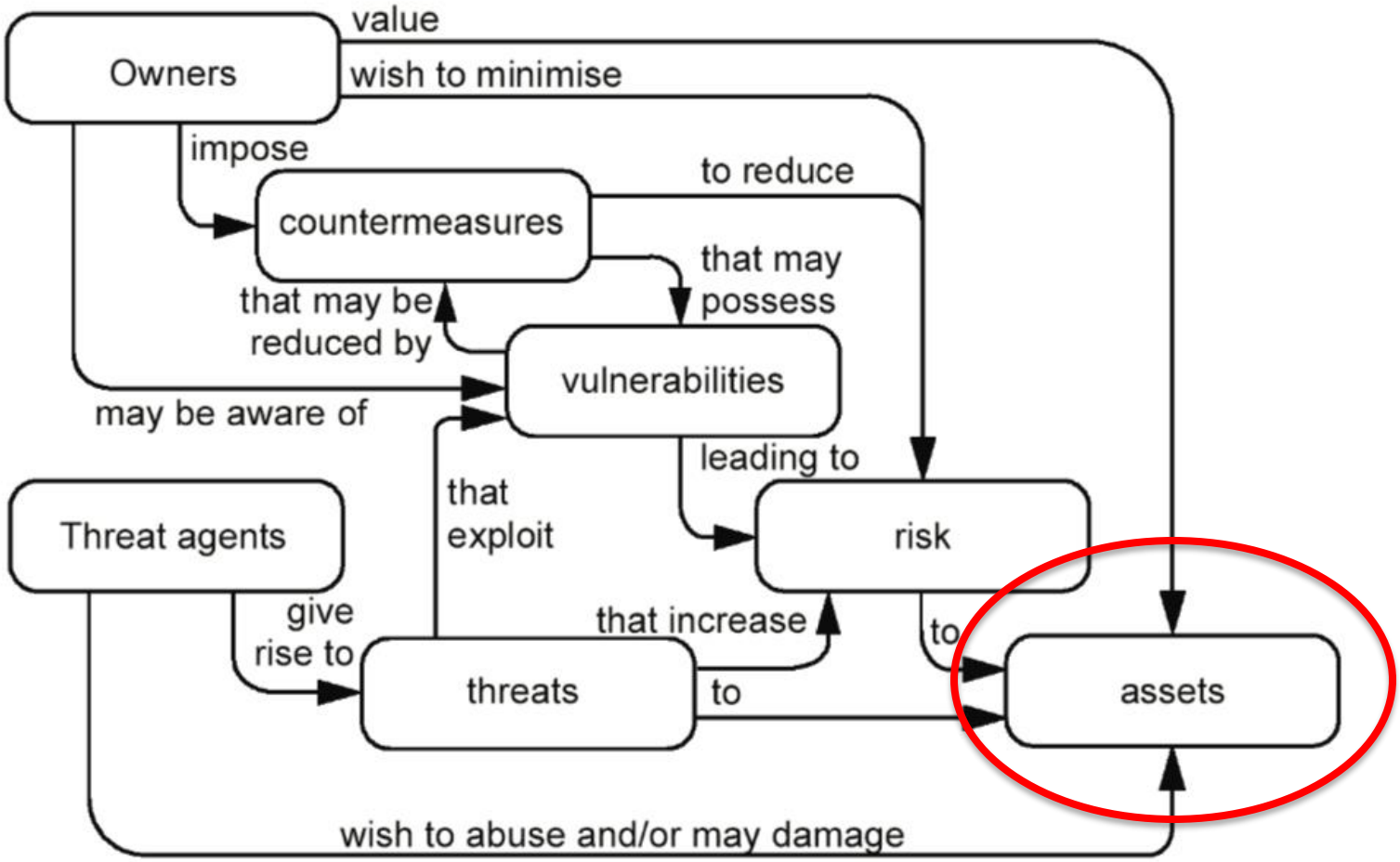
- 攻防双方都要平衡成本与收益
- 让对手付出更高的代价/成本

- 实例：某电商与薅羊毛产业的对抗
  - 羊毛党的成本：养号
  - 电商防范的成本：安全团队

作为企业安全的管理者，安全从何入手？



风险分析模型（Threat Modeling



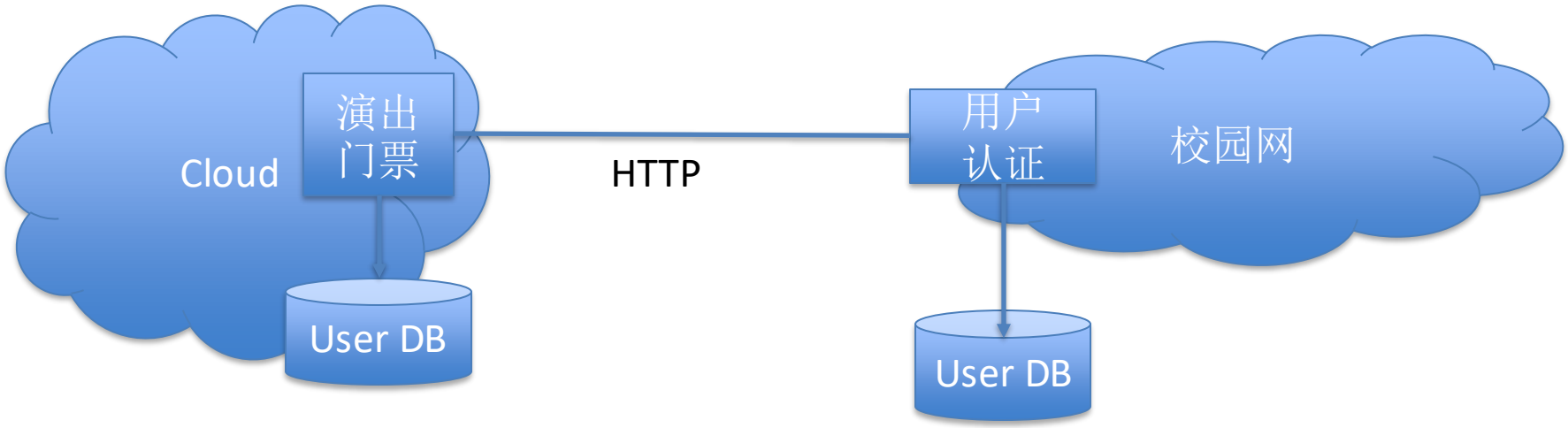
Common Criteria, for Information Technology Security Evaluation
https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf

首先要明确保护的资产（Asset）

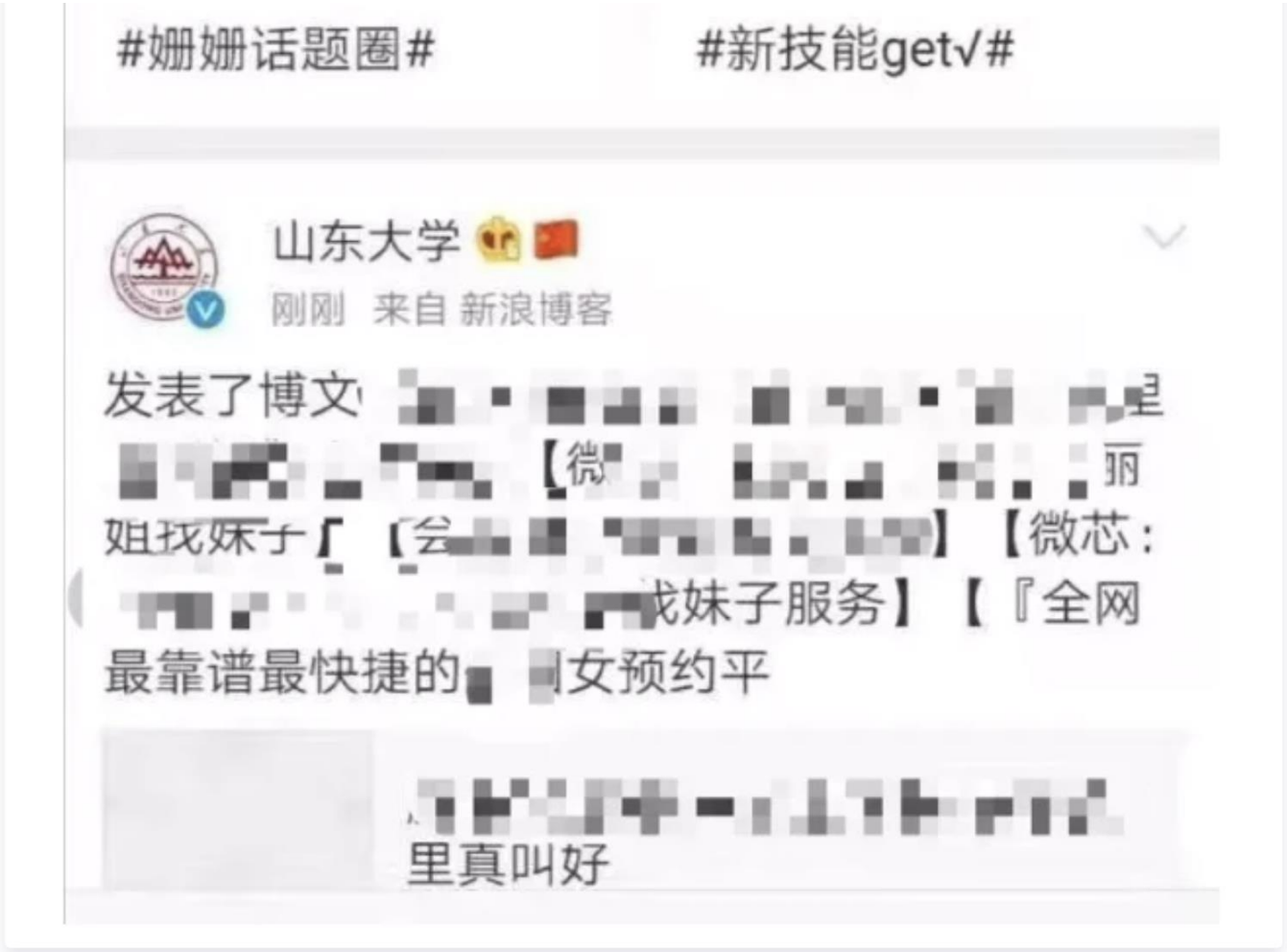
- Personal asset
  - Hardware, software, data
  - Bank/shopping accounts, …
  - Content stored, transmitted over networks, Cloud…
- Enterprise asset:
  - IT infrastructure, business plan, payroll …
  - Business information: user info, credit card,…
  - Intellectual property
  - Service: web server, reputation (deface) ….
- ISP
  - Network resource: link bandwidth

校园网信息安全的一个案例

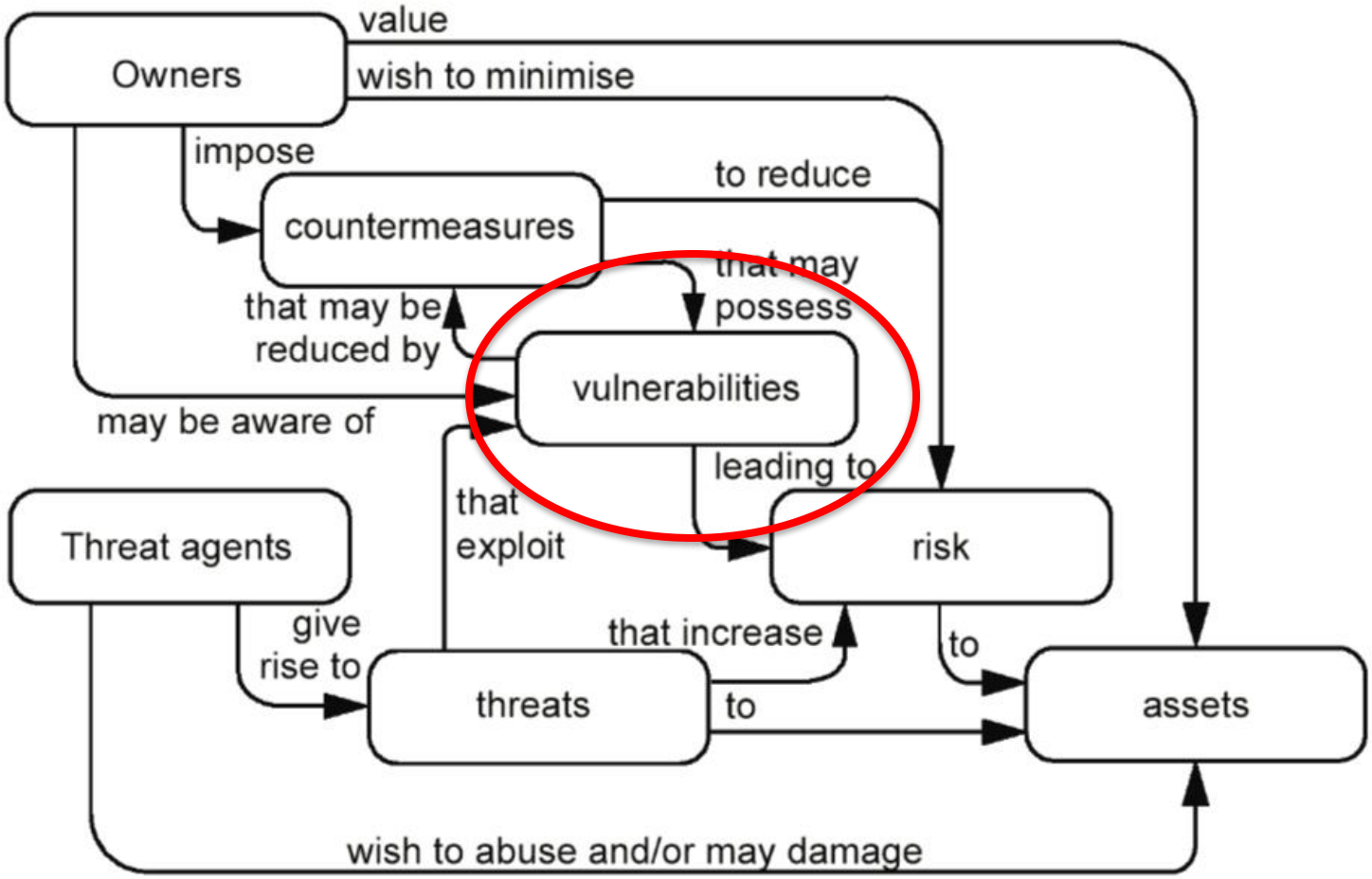
- 你的账号信息在哪里存储、传输？



信息资产：社交媒体账号


#姗姗话题圈#
#新技能get√#
山东大学
刚刚 来自 新浪博客
发表了博文
【微
丽
姐找妹子【 【会
】【微芯：
找妹子服务】【『全网
最靠谱最快捷的 女预约平
里真叫好

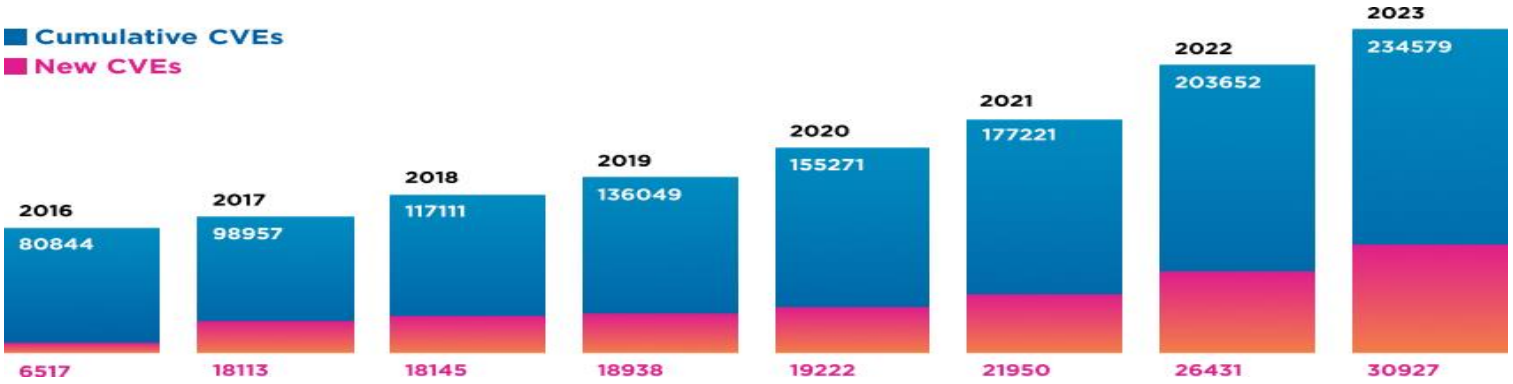
Threat Modeling



Common Criteria, for Information Technology Security Evaluation
https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf

安全漏洞（Vulnerability）

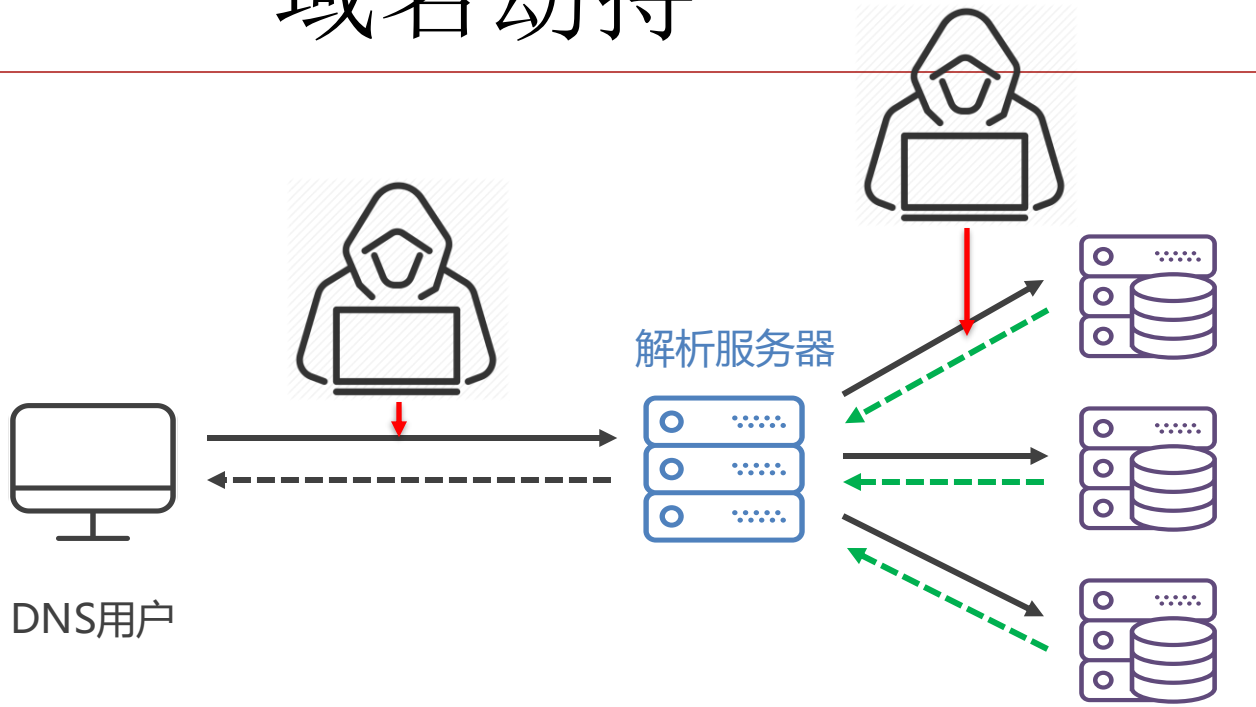
- 什么是漏洞
  - 信息系统在设计、实现和使用过程中出现的错误，攻击者可以利用这些错误破坏系统的安全属性（保密性、完整性、可用性、非授权使用等）
- 为什么漏洞那么多
  - 计算机软件和硬件复杂，如，通常每10行代码1 个错误
  - 由于时间紧张，软件测试不足
  - 应用场景发生变化，比如移动电话主要功能不是电话
  - 技术发生了变化，MD5 算法2003 年被破解

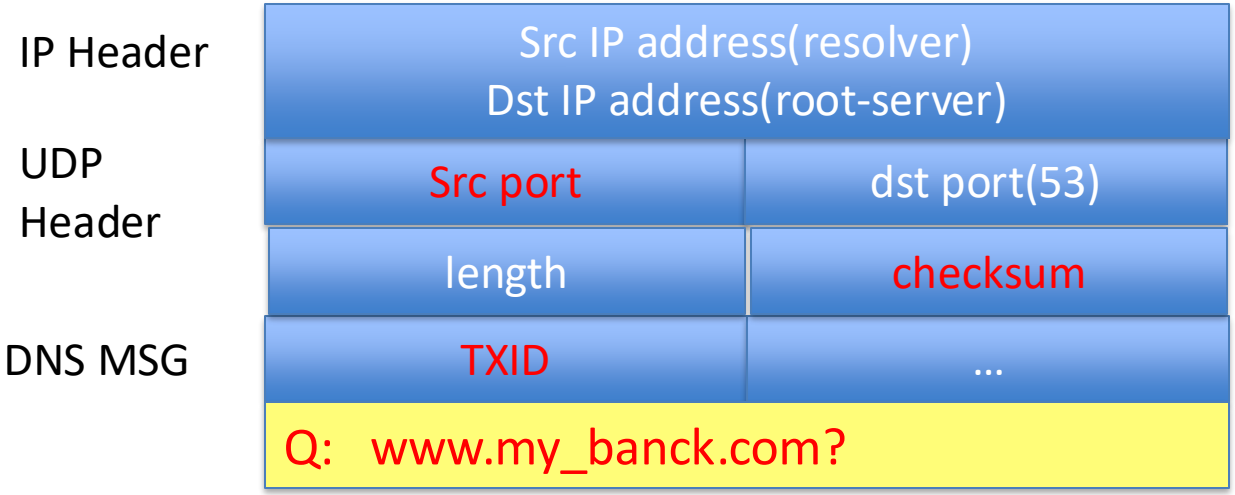


安全漏洞（Vulnerability）

- 协议设计或结构设计漏洞
  - 逻辑缺陷和设计漏洞
  - 例：米特尼克利用的 TCP 序列号可预测
- 软件实现漏洞
  - 软件实现的漏洞
  - 举例：输入验证的不足导致内存越界/溢出；
- 配置漏洞
  - 出厂配置、弱口令、多个系统相同的口令
- 人的弱点
  - 同情心、恐惧心理
  - 安全意识不足

域名劫持


解析服务器
DNS用户
权威服务器


IP Header
Src IP address(resolver)
Dst IP address(root-server)
UDP Header
Src port
dst port(53)
length
checksum
DNS MSG
TXID
...
Q: www.my_banck.com?

域名解析被劫持的实例

dig @<name_server> <domain_name> 或 nslookup <domain_name> <name_server>

```
[duanhx@ccert ~]$ dig @www.mit.edu twitter.com

; <<>> DiG 9.11.0-P1 <<>> @www.mit.edu twitter.com
; (3 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45230
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;twitter.com.                   IN      A

;; ANSWER SECTION:
twitter.com.            94      IN      A       8.7.198.45

;; Query time: 101 msec
;; SERVER: 23.77.14.148#53(23.77.14.148)
```

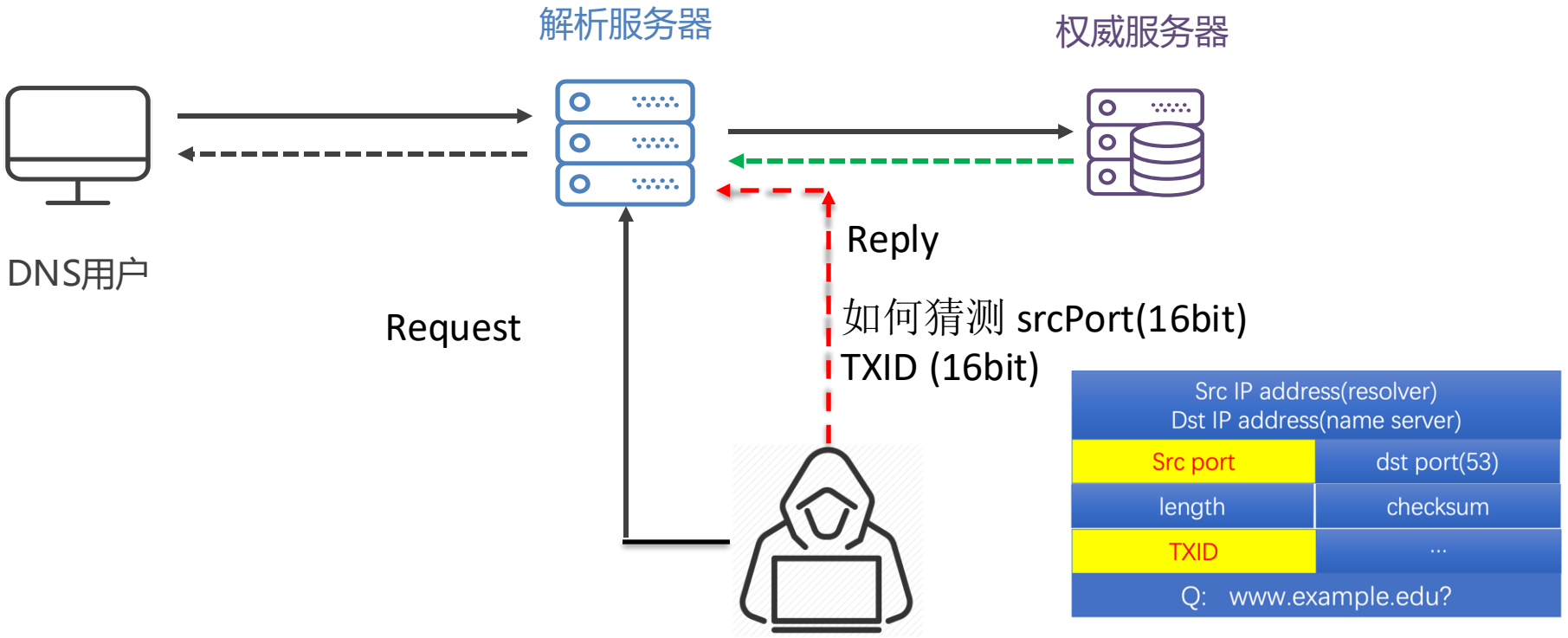
北京联通的家庭宽带

- 网关:192.168.1.1，我的地址： 192.168.1.2
- $ dig @2.0.0.0 www.tsinghua.edu.cn

```
west-2-w.amazonaws.com., s3-us-west-2-w.amazonaws.com. A 52.218.208.42 (98)
22:05:20.584552 IP (tos 0x0, ttl 64, id 33383, offset 0, flags [none], proto UDP (17), length 88)
    192.168.1.2.61909 > 2.0.0.0.53: 48284+ [1au] A? www.tsinghua.edu.cn. (60)
22:05:20.591687 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 101)
    2.0.0.0.53 > 192.168.1.2.61909: 48284 2/0/0 www.tsinghua.edu.cn. CNAME www.d.tsinghua.edu.cn., ww
w.d.tsinghua.edu.cn. A 166.111.4.100 (73)
22:05:22.208711 IP (tos 0x0, ttl 64, id 34618, offset 0, flags [none], proto UDP (17), length 88)
    192.168.1.2.63681 > 2.0.0.0.53: 30294+ [1au] A? www.tsinghua.edu.cn. (60)
22:05:22.214248 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 104)
    2.0.0.0.53 > 192.168.1.2.63681: 30294- 1/0/1 . OPT UDPsize=4096 (76)
22:05:34.761471 IP (tos 0x0, ttl 64, id 51485, offset 0, flags [none], proto UDP (17), length 85)
    192.168.1.2.64851 > 2.0.0.0.53: 58336+ [1au] A? www.facebook.com. (57)
22:05:34.773709 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 78)
    2.0.0.0.53 > 192.168.1.2.64851: 58336 1/0/0 www.facebook.com. A 69.171.245.53 (50)
22:05:38.070274 IP (tos 0x0, ttl 64, id 43080, offset 0, flags [none], proto UDP (17), length 85)
    192.168.1.2.51905 > 2.0.0.0.53: 18130+ [1au] A? www.facebook.com. (57)
22:05:38.095749 IP (tos 0x0, ttl 64, id 0, offset 0, flags [DF], proto UDP (17), length 101)
    2.0.0.0.53 > 192.168.1.2.51905: 18130- 1/0/1 . OPT UDPsize=4096 (73)
```

Off Path 攻击

- 攻击者在无法监测链路的情况下，伪造DNS服务器的响应
- 缓存污染攻击(Cache Poisoning)



DNS的缓存污染漏洞

新的缓存污染方法

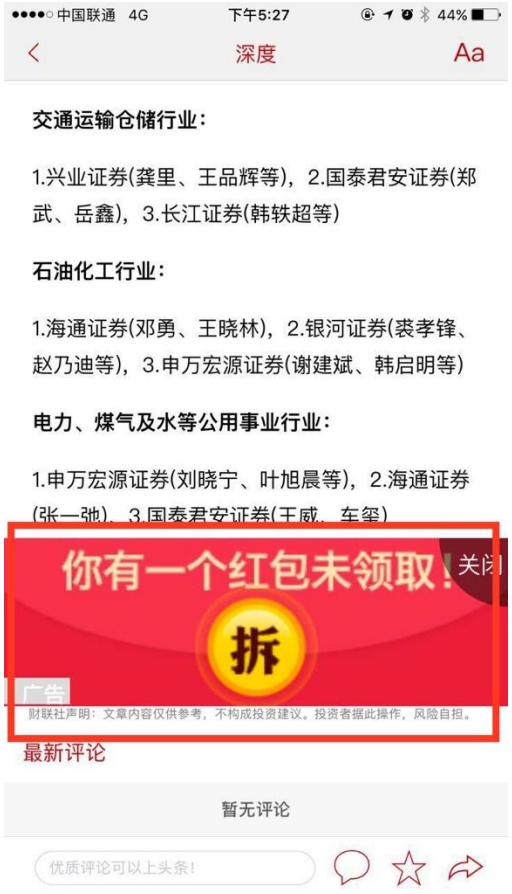
2019北京网络安全大会
2019 BEIJING CYBER SECURITY CONFERENCE

- 清华-奇安信联合实验室发现的新型DNS缓存污染攻击：构造超大的DNS请求，强迫服务器分片

小米 飞鱼星 ASUS D-Link TP-LINK Tenda 腾达 motorola
HUAWEI MERCURY 水星 MerCruiser LINKSYS WAVLINK 睿因 FAST 迅捷 gee 极路由

Lab2、DNS攻击实验
要达到的效果

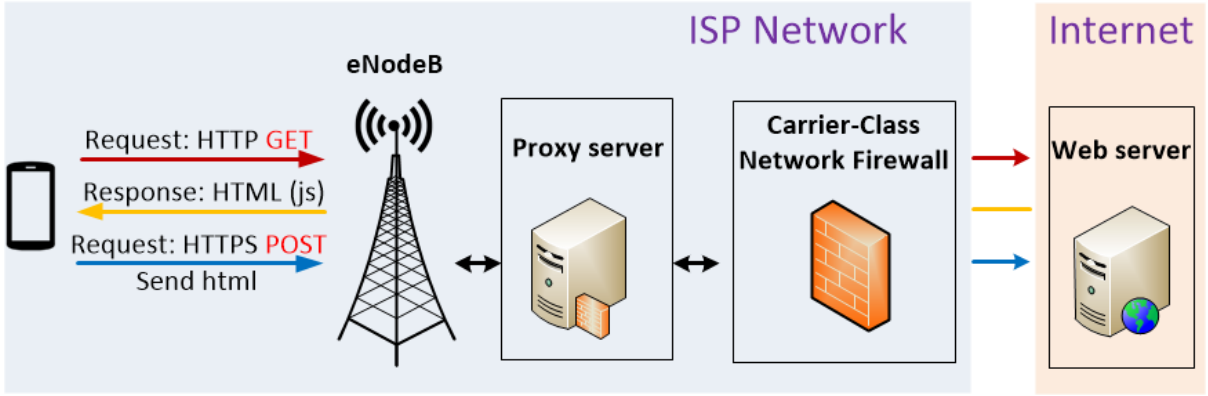
HTTP流量劫持


中国联通 4G 下午5:27 44%
深度 Aa
交通运输仓储行业：
1.兴业证券(龚里、王品辉等)，2.国泰君安证券(郑武、岳鑫)，3.长江证券(韩轶超等)
石油化工行业：
1.海通证券(邓勇、王晓林)，2.银河证券(裘孝锋、赵乃迪等)，3.申万宏源证券(谢建斌、韩启明等)
电力、煤气及水等公用事业行业：
1.申万宏源证券(刘晓宁、叶旭晨等)，2.海通证券
你有一个红包未领取！
关闭
拆
广告
财联社声明：文章内容仅供参考，不构成投资建议。投资者据此操作，风险自担。
最新评论
暂无评论
优质评论可以上头条！

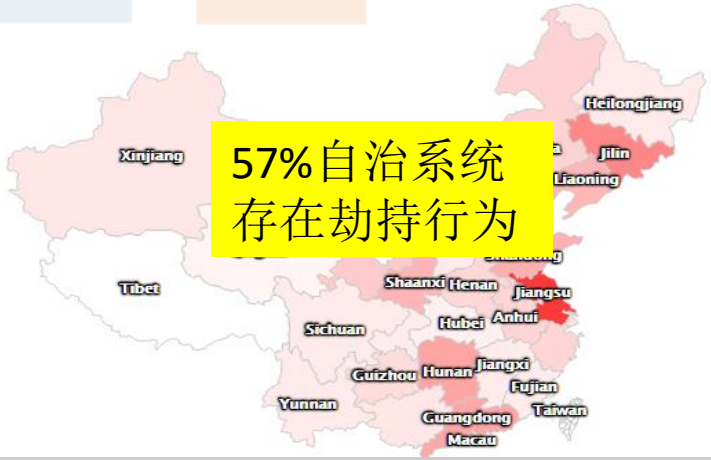

中国移动 上午5:47 99%
返回 杉易贷-公开透明，安全可靠...
杉易贷
www.33Lend.com
7月8日 一步到位
杉易贷新版网站7月8日正式上线
项目列表
杉易贷20151225001
投标中
年化利率 期限 金额
10.40% 6个月 800万
一次性还款
已完成34.86%
杉易贷20151225002
即将发布
年化利率 期限 金额
10.50% 1个月 300万
无码爽片在线看
日韩、欧美、内地万部大片在线观看
未成年人禁止点击 看片神器
关闭


14:23 4G 37
六公司关于抵制流量劫持等...
今日头条
3.5亿用户的选择
立即打开
六公司关于抵制流量劫持等违法行为的联合声明
今日头条 头条号
12-25 10:06
套餐推荐
尊敬的客户： 根据您的流量使用情况
推荐您订购: 神州行畅听卡和4G套餐128元档 含国内流量1G,国内主叫420分钟,国内接听免费。订购成功后，现有主套餐将被替换为神州行畅听卡和4G套餐128元档,下月生效。发送短信8888或6666到10086可查询现在已办理的套餐.
以后提醒
立即订购
下，流量劫持方式主要分为两类：

国内移动网络中隐私泄露



测试规模	数量	发生劫持
HTTP 会话数	33,439	1,291 (3.9%)
IP地址	30,810	451 (1.5%)
省	31	30 (97%)
自治系统（AS）	79	45 （57%）

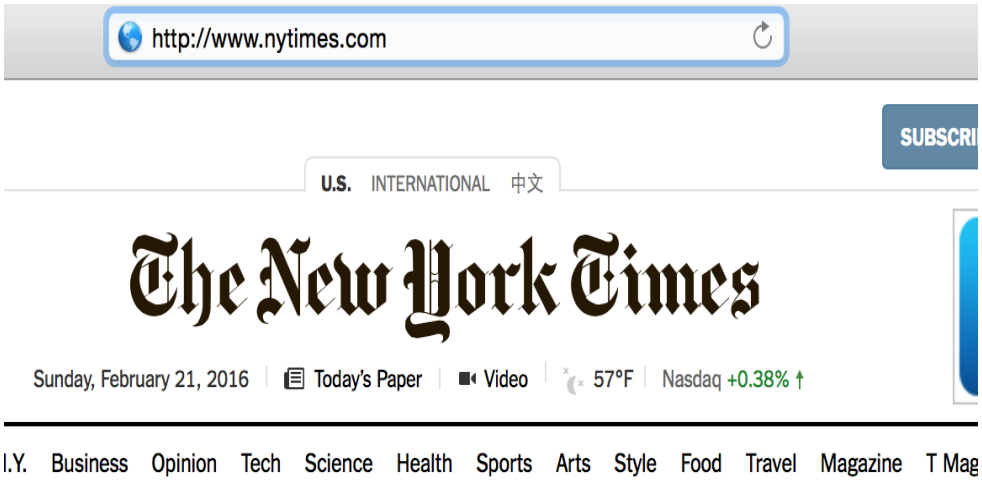


Mingming Zhang, Baojun Liu, Chaoyi Lu, Jia Zhang, Shuang Hao, Haixin Duan. Measuring Privacy Threats in China-Wide Mobile Networks. 8th USENIX Workshop on Free and Open Communications on the Internet(FOCI), 2018

加密的协议就安全了，如HTTPS？

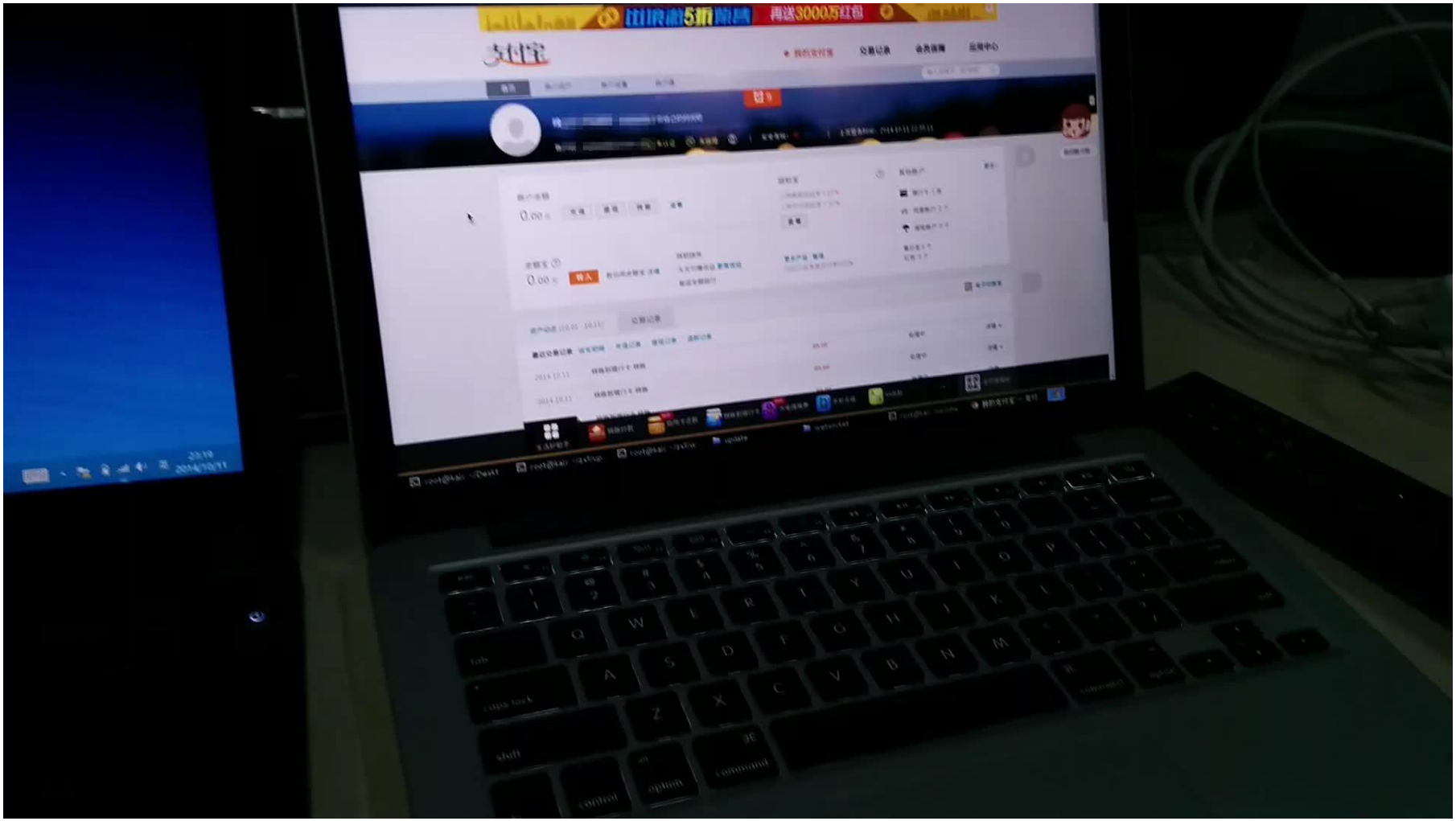
Surfing Internet with Public Wi-Fi

No sensitive application



Weeks later, in a safe network…

演示：谁动了你的电子钱包



Affected website and browsers

郑晓峰、杨坤等获GeekPwn15第一、三，共78万奖金

第三名：杨坤　　第一名：郑晓峰等

漏洞（Vulnerabilities）

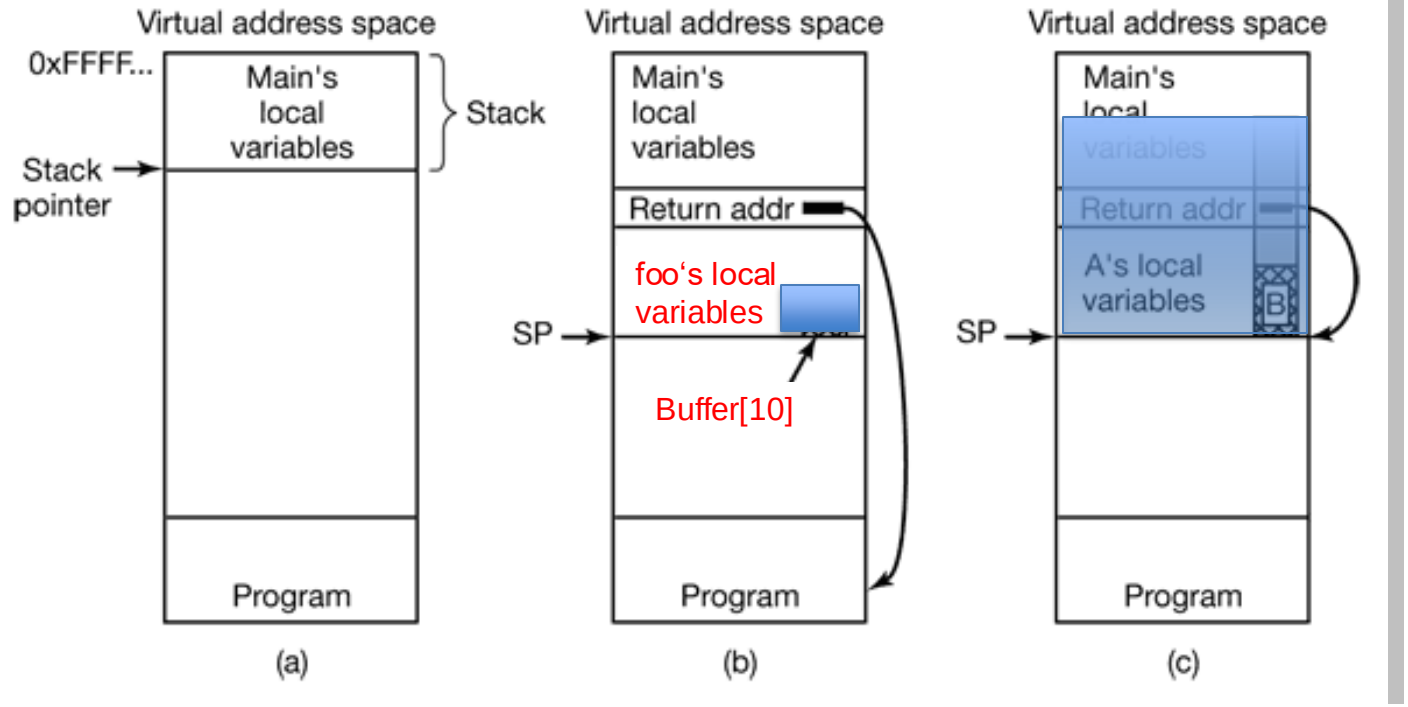
- 设计阶段的漏洞，例如
  - DNS和HTTP明文传输，没有加密、认证
- 实现阶段的漏洞
  - Buffer Overwriet (Overflow)
  - Buffer Overread (HeartBleed)
- 部署或配置阶段的漏洞
  - 熟悉的中间人攻击

这段代码有什么问题？

```
 1 #include <stdio.h>
 2 #include <string.h>
 3
 4 void foo(const char * input){
 5     int i;
 6     char buffer[10];
 7
 8     strcpy(buffer, input);
 9     printf("%s\n", buffer);
10     for (i=0; i<=10; i++)
11         buffer[i]=input[i];
12     printf("%s\n", buffer);
13 }
14
15 int main(int argc, char * argv[]){
16
17     if( argc != 2) {
18         printf("Usage: %s <input> \n", argv[0]);
19         return -1;
20     }
21     foo(argv[1]);
22     return 0;
23 }
```

这段代码有什么问题？

```
1 #include <stdio.h>
2 #include <string.h>
3
4 void foo(const char * input){
5     int i;
6     char buffer[10];
7
8     strcpy(buffer, input);
9     printf("%s\n", buffer);
```



这段代码有什么问题？

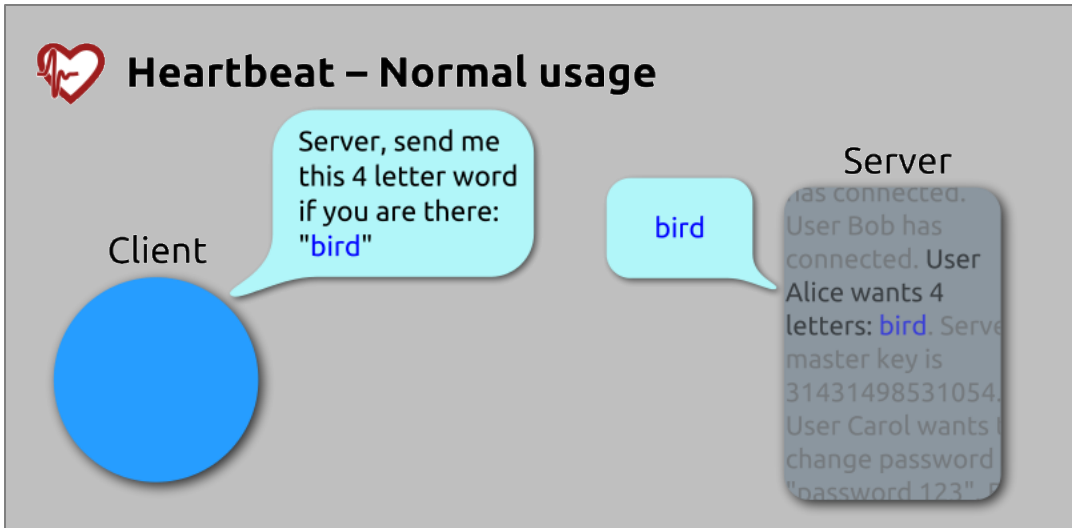
```
 1 #include <stdio.h>
 2 #include <string.h>
 3
 4 void foo(const char * input){
 5     int i;
 6     char buffer[10];
 7
 8     strcpy(buffer, input);
 9     printf("%s\n", buffer);
10     for (i=0; i<=10; i++)
11         buffer[i]=input[i];
12     printf("%s\n", buffer);
13 }
14
15 int main(int argc, char * argv[]){
16
17     if( argc != 2) {
18         printf("Usage: %s <input> \n", argv[0]);
19         return -1;
20     }
21     foo(argv[1]);
22     return 0;
23 }
```

漏洞（Vulnerabilities）

- 设计阶段的漏洞，例如
  - 路由转发不验证源地址
  - DNS和HTTP明文传输
- 实现阶段的漏洞
  - 缓冲区溢出（Buffer Overflow）
  - OpenSSL 的心脏出血漏洞（Heart Bleed）

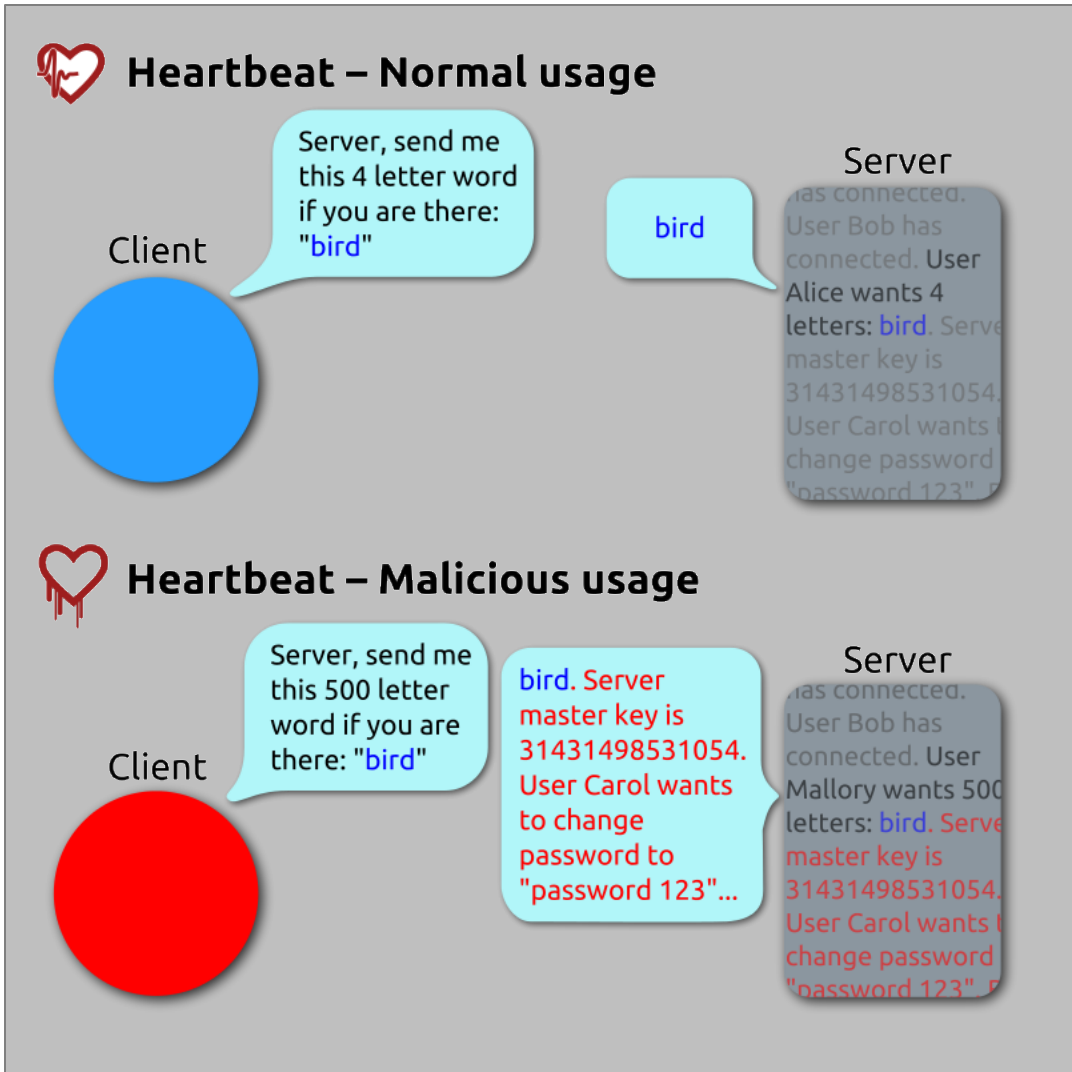
HeartBleed Bug(CVE-2014-0160)

- Implementation bug of OpenSSL library
- TLS/DTLS
- Heartbeat Extension

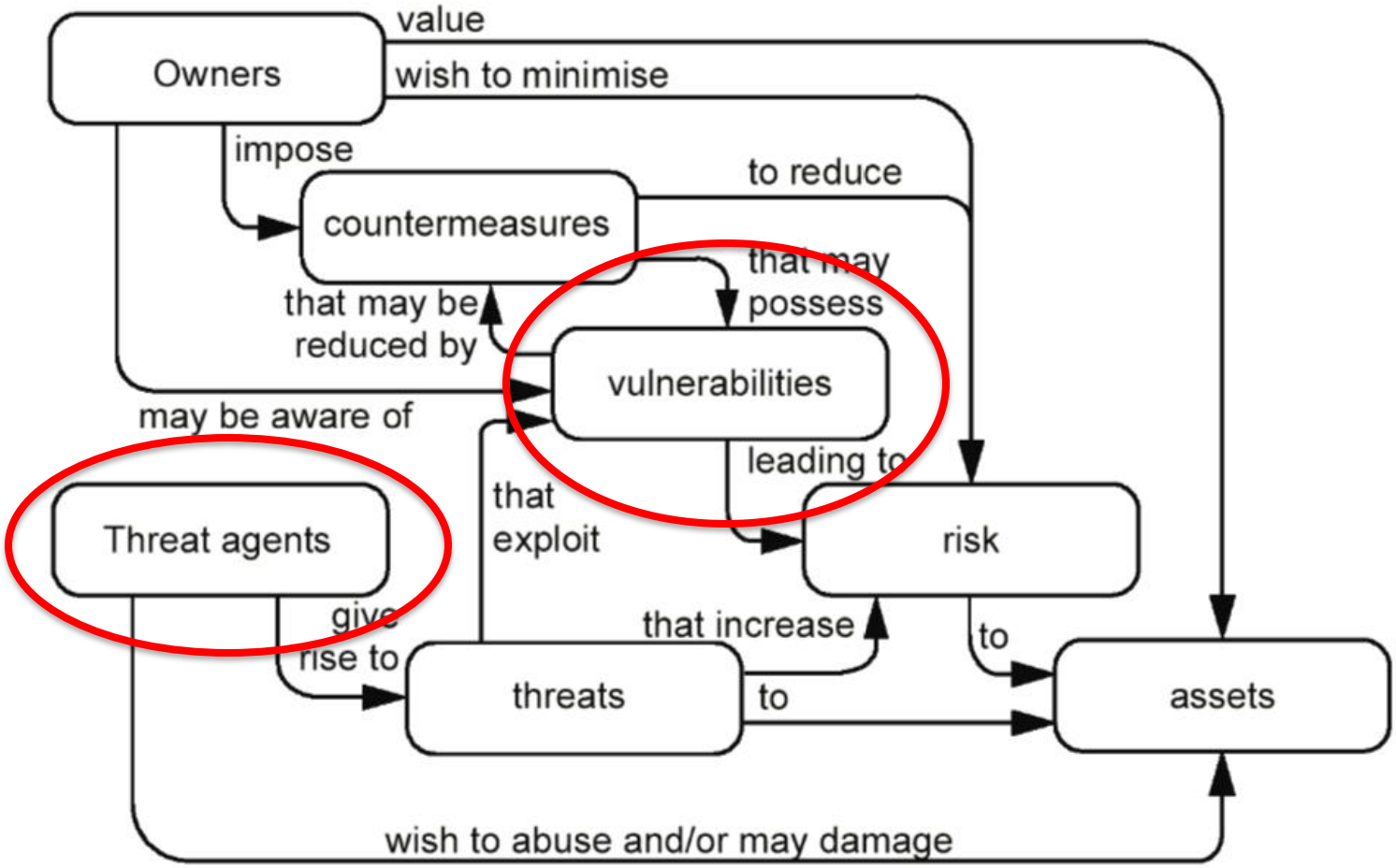


HeartBleed Bug(CVE-2014-0160)

- Implementation bug of OpenSSL library
- TLS/DTLS
- Heartbeat Extension



风险分析模型（Threat Modeling

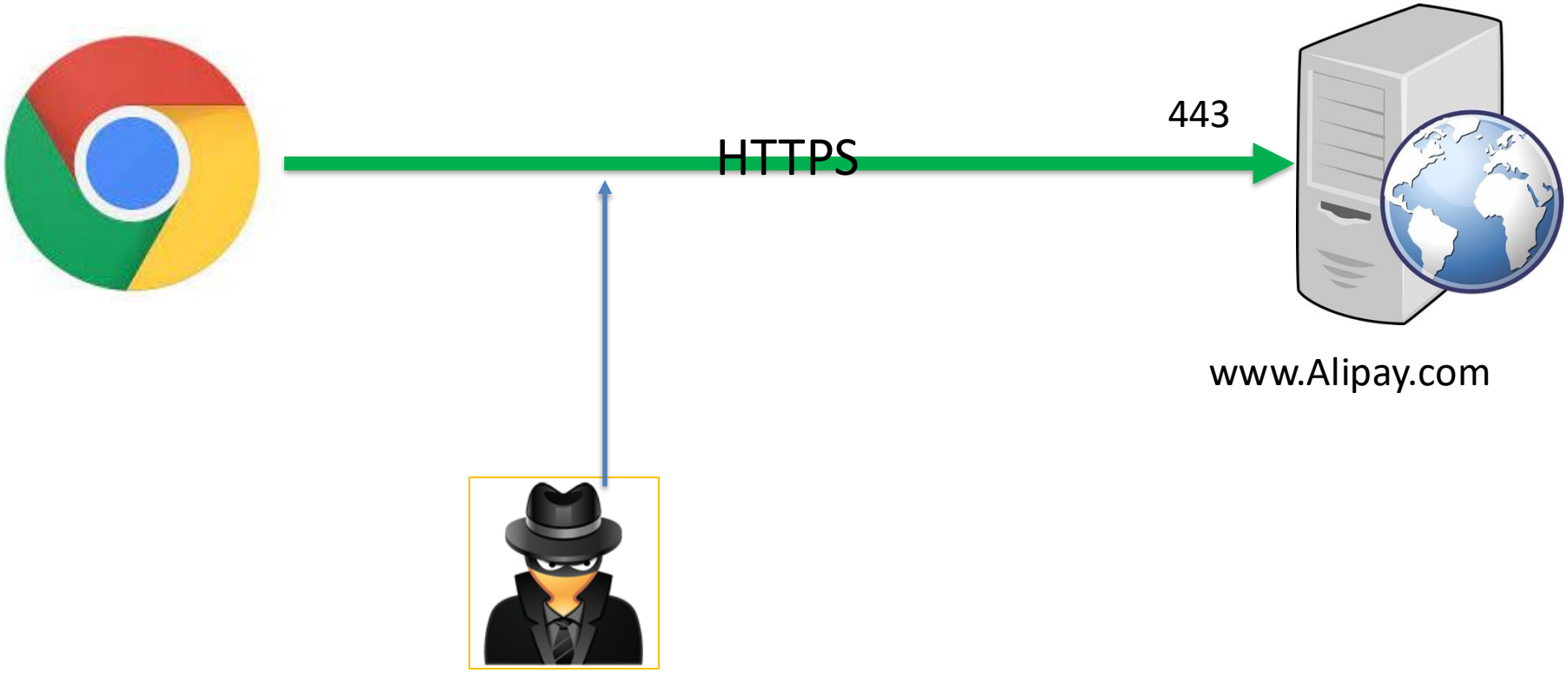


Common Criteria, for Information Technology Security Evaluation
https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf

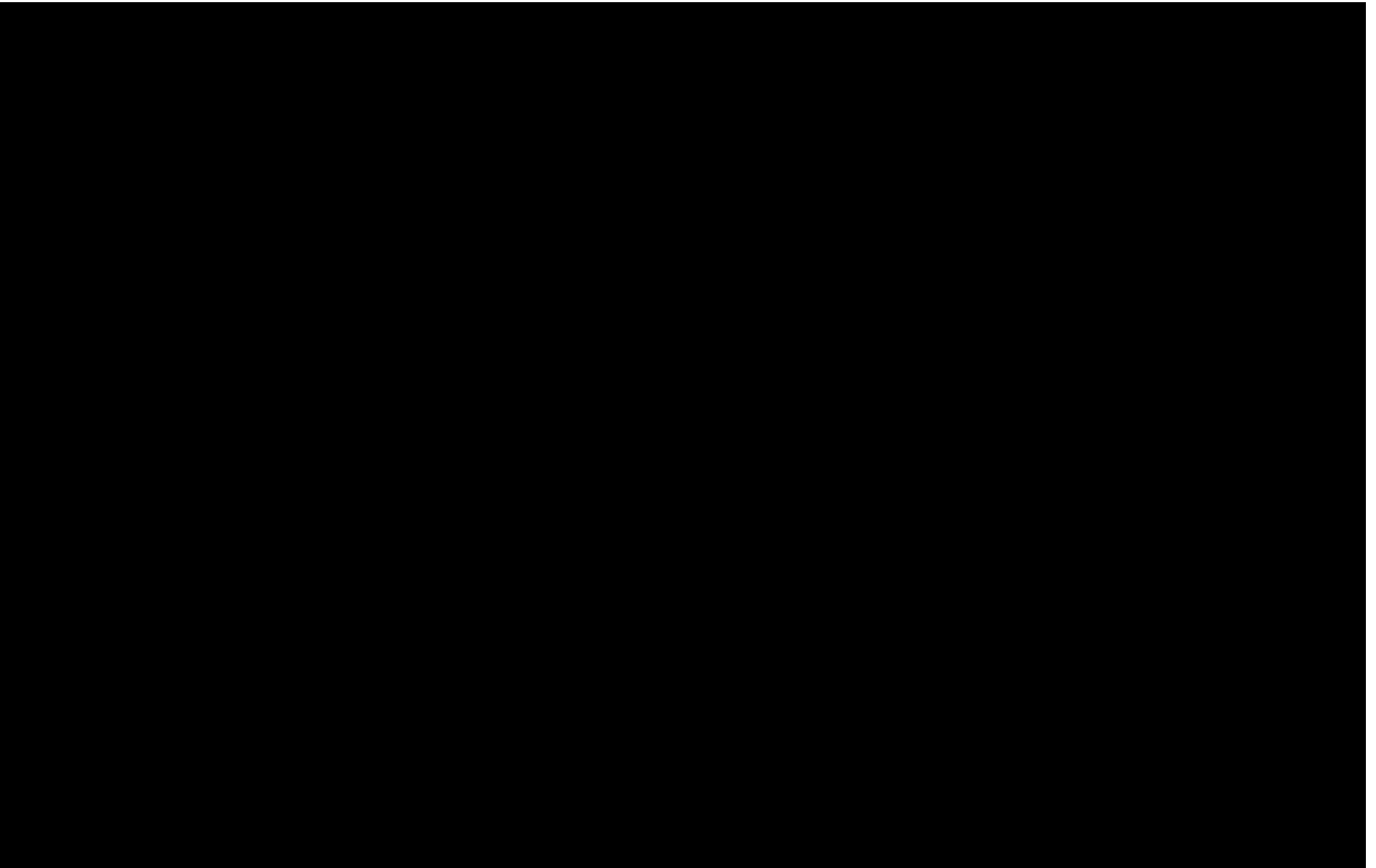
漏洞（Vulnerabilities）

- 设计阶段的漏洞，例如
  - DNS和HTTP明文传输，没有加密、认证
- 实现阶段的漏洞
  - HeartBleed 漏洞攻击
  - Host of Troubles攻击
- 部署或配置阶段的漏洞
  - 弱口令/缺省口令
  - 实例：自签名根证书

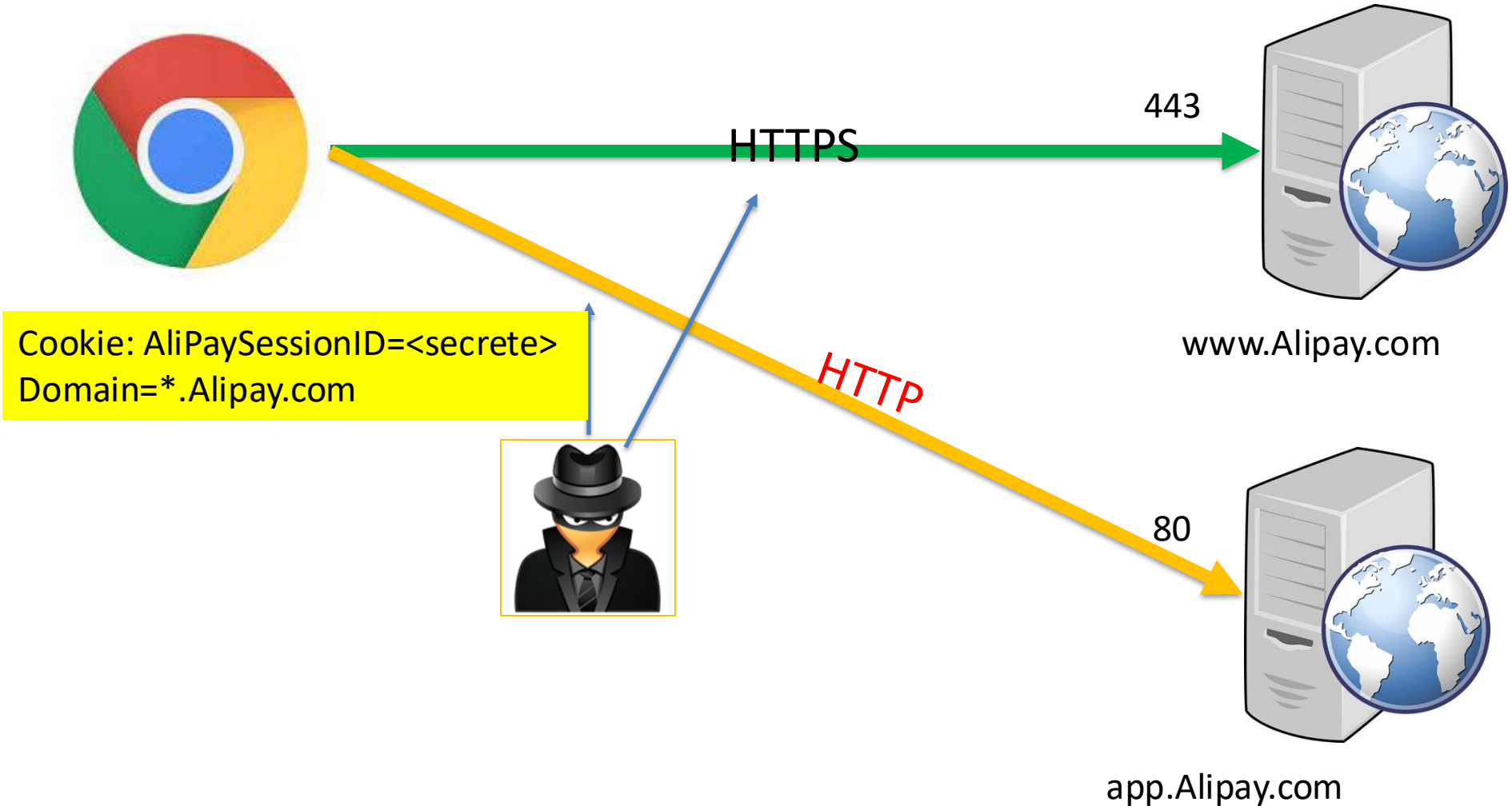
HTTPS和HTTP混合部署问题



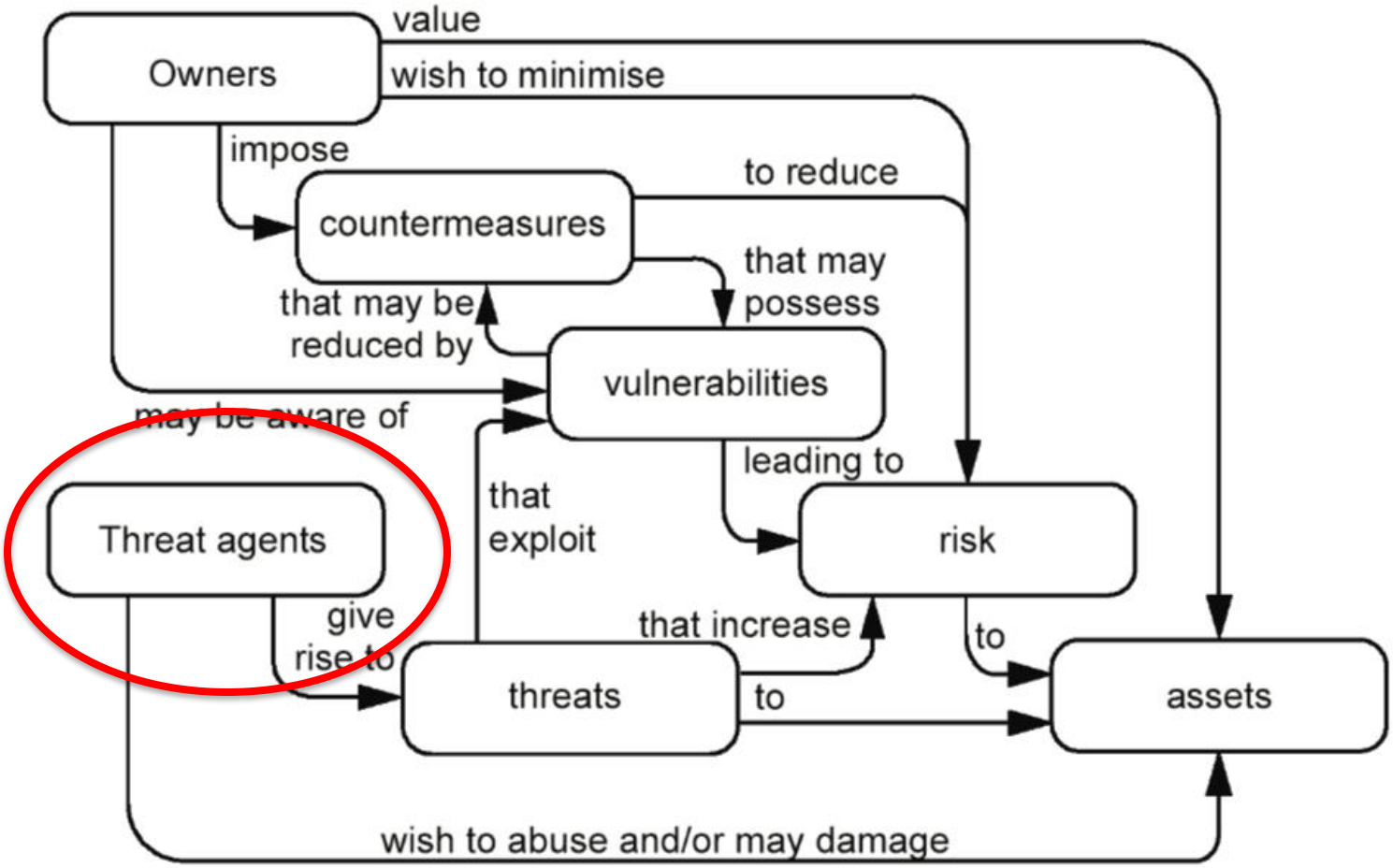
Deploy problem: session hijacking



HTTPS和HTTP混合部署问题



Threat Modeling



Common Criteria, for Information Technology Security Evaluation
https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf

攻击者是谁（Threat Agent）

敌手（Adversary）

- 脚本小子（Script Kiddie）
- Hackers for fun
- 网络犯罪
- 黑客行为主义者 (Hacktivism)
- 商业竞争对手
- 国家支持的黑客
- …

第一个大规模安全事件：莫里斯蠕虫(1988)

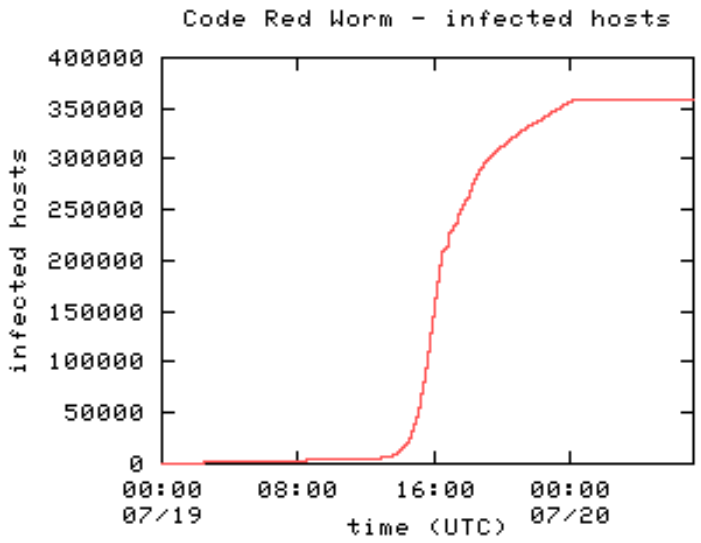
- 罗伯特·泰潘·莫里斯（Robert Tappan Morris)， 1988 年哈佛大学毕业后在 Cornell 大学计算机读研究生
- 1988 年编写莫里斯蠕虫感染互联网 10%的电脑（6,000），导致互联网瘫痪。美国《计算机欺诈和滥用法》颁布后第一个被判重刑（三年缓刑，400 H 社区服务，$10,050罚款
- 美国企业家，计算机科学家，MIT 教授，美国工程院院士

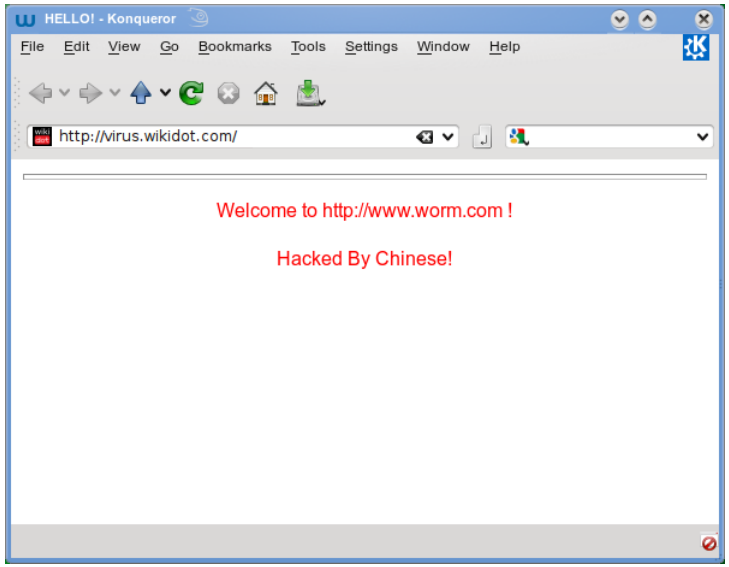
莫里斯蠕虫利用的漏洞
• 操作系统的弱口令 • 远程登录服务的信任主机列表 • UNIX Sendmail 程序的调试模式漏洞 • 网络服务Fingerd的缓冲区溢出漏洞

Hackers for Fun, Code Red, I & II, 2001

- Virus, Worm, DoS, …
  - Morris Worm(1988)
  - Code Red, I & II, 2001

```
GET /default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNN
%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801
%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190%u00c3
%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a  HTTP/1.0
```





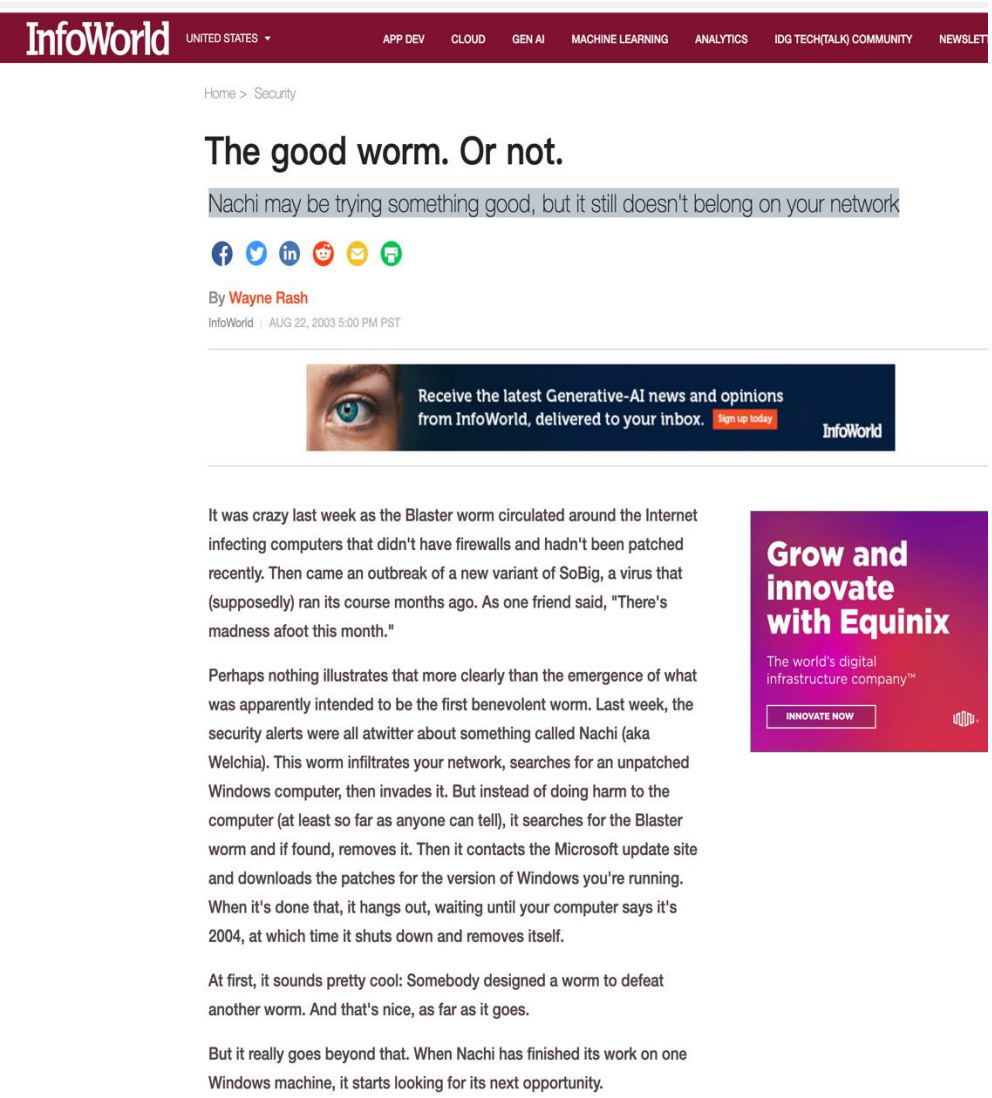
http://www.eeye.com/Resources/Security-Center/Research/Security-Advisories/AL20010717

http://www.caida.org/publications/papers/2002/codered/codered.pdf

2003年的冲击波蠕虫Blaster事件

- 2003年5月，微软发布了两个补丁，没有细节
- 2003 年 7 月， Xfocus发布漏洞利用的概念验证代码（POC），美国黑客完善这个POC
- 2003 年 8 月 11 日，利用该漏洞的蠕虫 Blaster 开始在网上快速传播
- 2003 年 8 月 15 日，40 万台计算机感染，开始对微软补丁更新服务进行 DOS 攻击
- 2003 年 8 月 18 日，冲击波杀手蠕虫大规模传播、导致大量网络拥塞
- 2004 年1 月，冲击波杀手自杀（Nachi）

Welchia(Nachi worm): Good worm?



InfoWorld UNITED STATES APP DEV CLOUD GEN AI MACHINE LEARNING ANALYTICS IDG TECH(TALK) COMMUNITY NEWSLET

Home > Security

The good worm. Or not.

Nachi may be trying something good, but it still doesn't belong on your network

By Wayne Rash

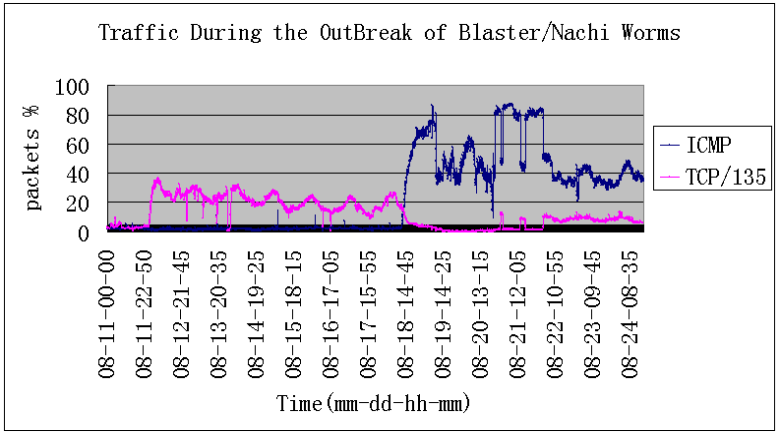
InfoWorld | AUG 22, 2003 5:00 PM PST

It was crazy last week as the Blaster worm circulated around the Internet infecting computers that didn't have firewalls and hadn't been patched recently. Then came an outbreak of a new variant of SoBig, a virus that (supposedly) ran its course months ago. As one friend said, "There's madness afoot this month."

Perhaps nothing illustrates that more clearly than the emergence of what was apparently intended to be the first benevolent worm. Last week, the security alerts were all atwitter about something called Nachi (aka Welchia). This worm infiltrates your network, searches for an unpatched Windows computer, then invades it. But instead of doing harm to the computer (at least so far as anyone can tell), it searches for the Blaster worm and if found, removes it. Then it contacts the Microsoft update site and downloads the patches for the version of Windows you're running. When it's done that, it hangs out, waiting until your computer says it's 2004, at which time it shuts down and removes itself.

At first, it sounds pretty cool: Somebody designed a worm to defeat another worm. And that's nice, as far as it goes.

But it really goes beyond that. When Nachi has finished its work on one Windows machine, it starts looking for its next opportunity.

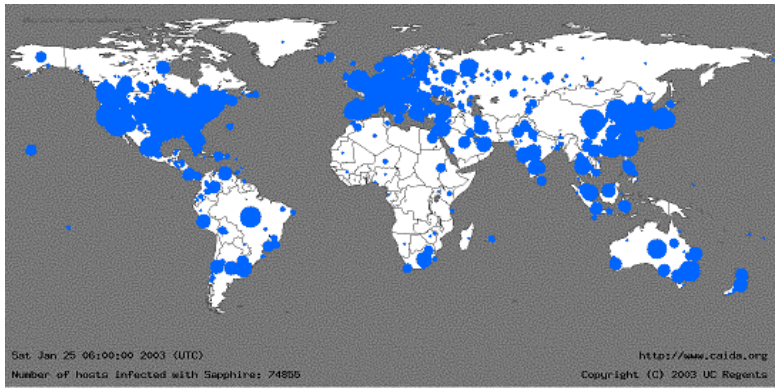


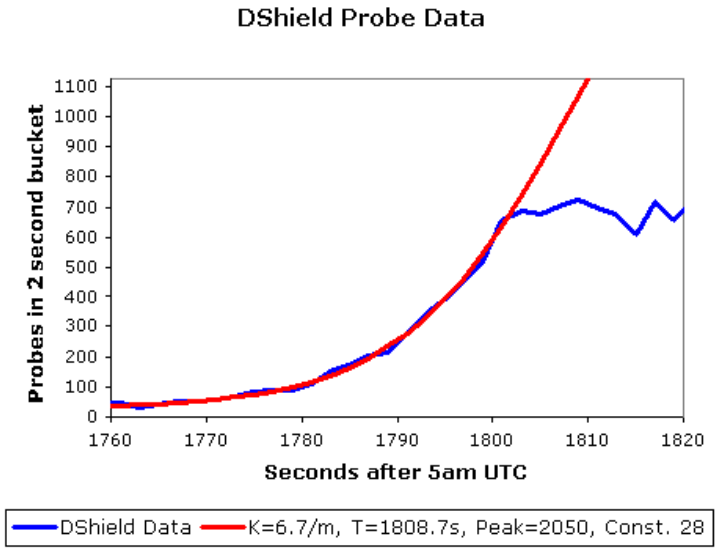
Slammer worm (2003)

- Virus, Worm, DoS, …
  - Morris Worm(1988)
  - Code Red, I & II, 2001
  - Blaster, Slammer(2003)

传播太快，把网络堵了

10分钟感染全球90%





http://cseweb.ucsd.edu/~savage/papers/IEEESP03.pdf

https://www.caida.org/publications/papers/2003/sapphire/sapphire.html

黑客行为主义者 (Hacktivism)

NEWS HOME NEWS EVENTS PROGRAMS SPACES PARTNER WITH US

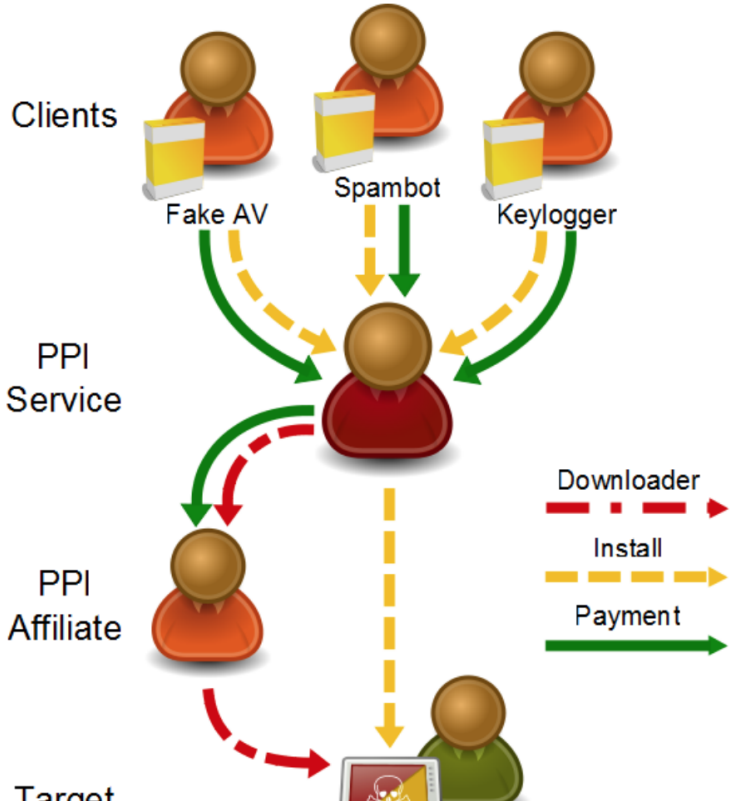
is ON! Join us at TNW Conference 2021 in Amsterdam for face-to-face business!

Anonymous Responds to SOPA: We'll Deface The Internet In Protest

Hackers for profit

PPI Ecosystem

- Clients
  - Pay the PPI
  - Want malware installed
  - Spambots, information harvesting, rootkits, fake AV
- Pay-per-install (PPI)
  - Purchases compromised hosts from affiliates
  - Resells to clients
- Affiliates
  - Compromise machines
  - Execute the PPI's binary



Measuring *Pay-per-Install*: The Commoditization of Malware Distribution

Juan Caballero†, *Chris Grier**‡, *Christian Kreibich**‡, *Vern Paxson**‡
†*IMDEA Software Institute* **UC Berkeley* ‡*ICSI*
juan.caballero@imdea.org {*grier, vern*}*@cs.berkeley.edu* *christian@icir.org*

Threats(2)： Hackers for profit

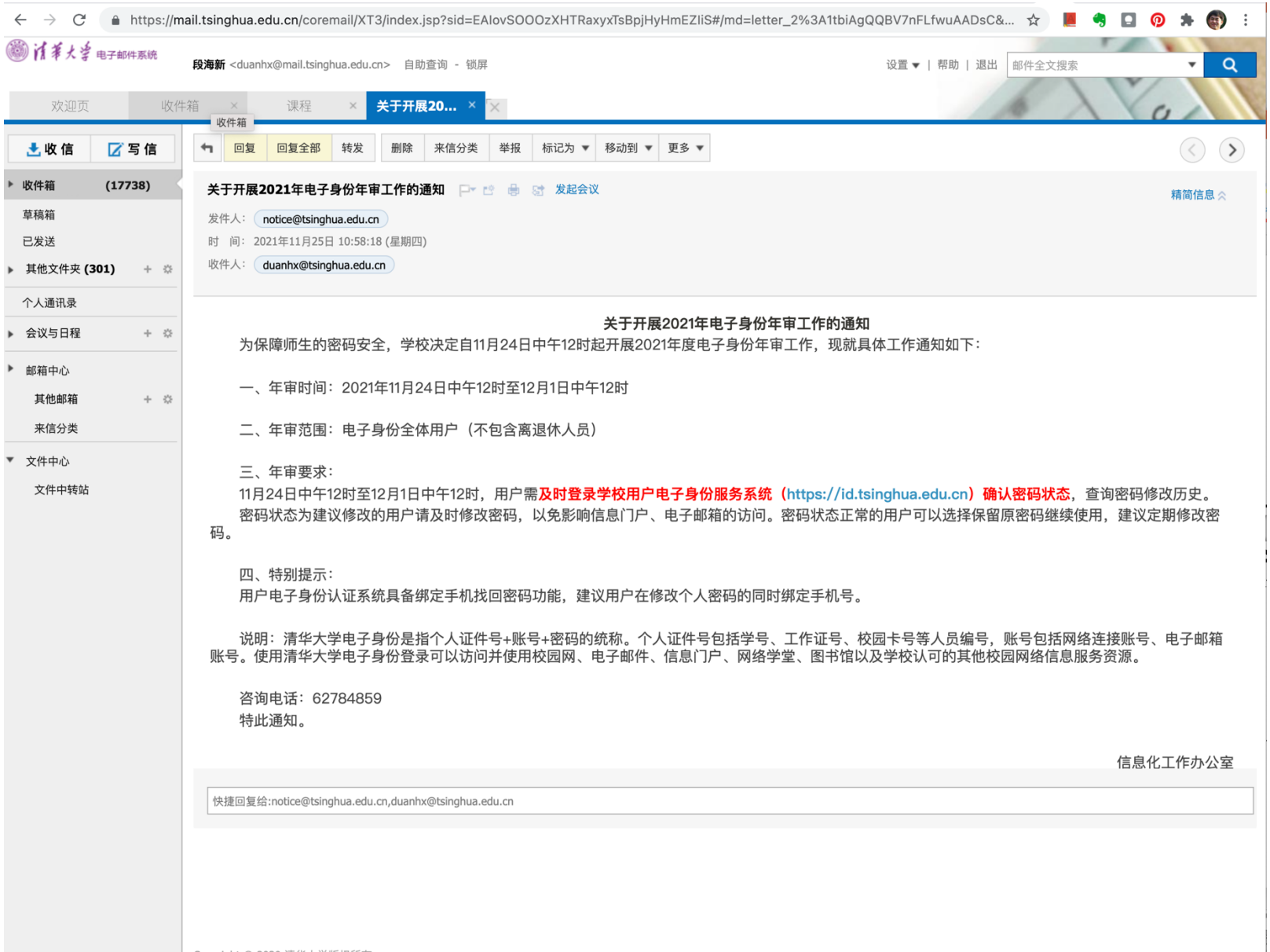
2017, WannaCry，感染150国200万

- 美国NSA泄露永恒之蓝漏洞利用
- 北朝鮮用来编制了勒索蠕虫？

勒索邮件


收件箱
垃圾邮件通知...
@tsi...
回复
回复全部
转发
删除
来信分类
举报
标记为
移动到
更多
@tsinghua.edu.cn password is
发起会议
发件人：
@tsinghua.edu.cn
(由 aaron@smith495.edu 代发)
真实发送地址与宣称的发件人地址不一致，
请谨慎审视邮件内容的真实性
时 间：2018年11月16日 15:47:33 (星期五)
收件人：
@tsinghua.edu.cn>
Hello there
I am a hacker who cracked your e-mail and device a few weeks back.
You typed in your pwd on one of the web sites you visited, and I intercepted this.

其实我们的攻击更专业一些...



攻击者是谁（Threat Agent）

敌手（Adversary）

- 合法用户
- 脚本小子（Script Kiddie）
- 网络犯罪
- 黑客行为主义者 (Hacktivism)
- 商业竞争对手
- **国家支持的黑客**
- …

Advanced Persistent Threats(APT)

- 强大的经济后盾、有序的组织
- 非常有经验的专业人员
- 目标：政府、商业或军事机构
- 目的：获取情报、商业机密、摧毁基础设施等
- 可以突破常规的安全防护，隐藏自己，以进行长期的攻击
- **多种入侵路径**（attack vector）

我经历的一次APT攻击

Re:公开征求对《网络数据安全标准体系建设指南》（征求意见稿）的意见 Inbox ×

KJBZ@...v.cn.mail-mfa.net Apr 17, 2020, 11:10 AM (3 days ago)

to tsinghua

KJBZ@miit.gov.cn
KJBZ@miit-gov.cn.mail-mfa.net
Add to Contacts

为落实《中华人[redacted]委员会关于加强网络信息保护的决定》《电信和互联网用[redacted]电信和互联网行业网络数据安全保护能力，充分发挥标[redacted]的引领和支撑作用，助力数字经济高质量发展，有关单位[redacted]（征求意见稿）及编制说明（见附件1、2）。

为进一步听取社会各界意见，现予以公示，公示日期截止2020年5月9日。如有意见或建议，请在公示期间填写《公示意见反馈信息表》（见附件3）并反馈至工业和信息化部科技司，电子邮件发送至KJBZ@miit.gov.cn（邮件主题注明：网络数据安全标准体系建设指南公示反馈）。

地址：北京市西长安街13号工业和信息化部科技司标准处

邮编：100846

联系电话：010-68205241

公示时间：2020年4月10日-2020年5月9日

Reply Forward

Re:公开征求对《网络数据安全标准体系建
稿）的意见 Inbox ×

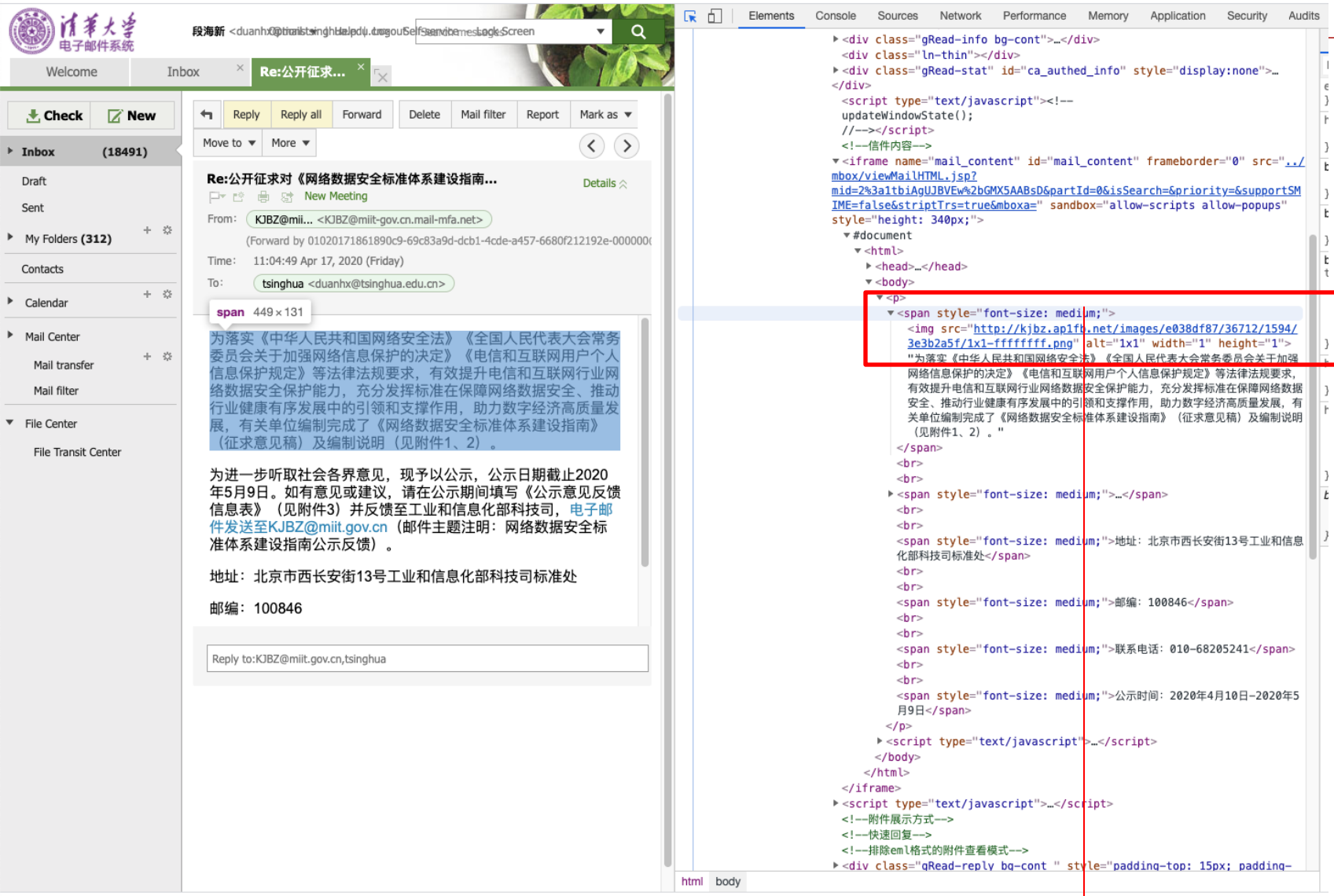
KJBZ@...v.cn.mail-mfa.net Fri, Ap

to tsinghua

为落实《中华人民共和国网络安全法》《全国人民代表大
决定》《电信和互联网用户个人信息保护规定》等法律法
络数据安全保护能力，充分发挥标准在保障网络数据安全
撑作用，助力数字经济高质量发展，有关单位编制完成了
（征求意见稿）及编制说明（见附件1、2）。

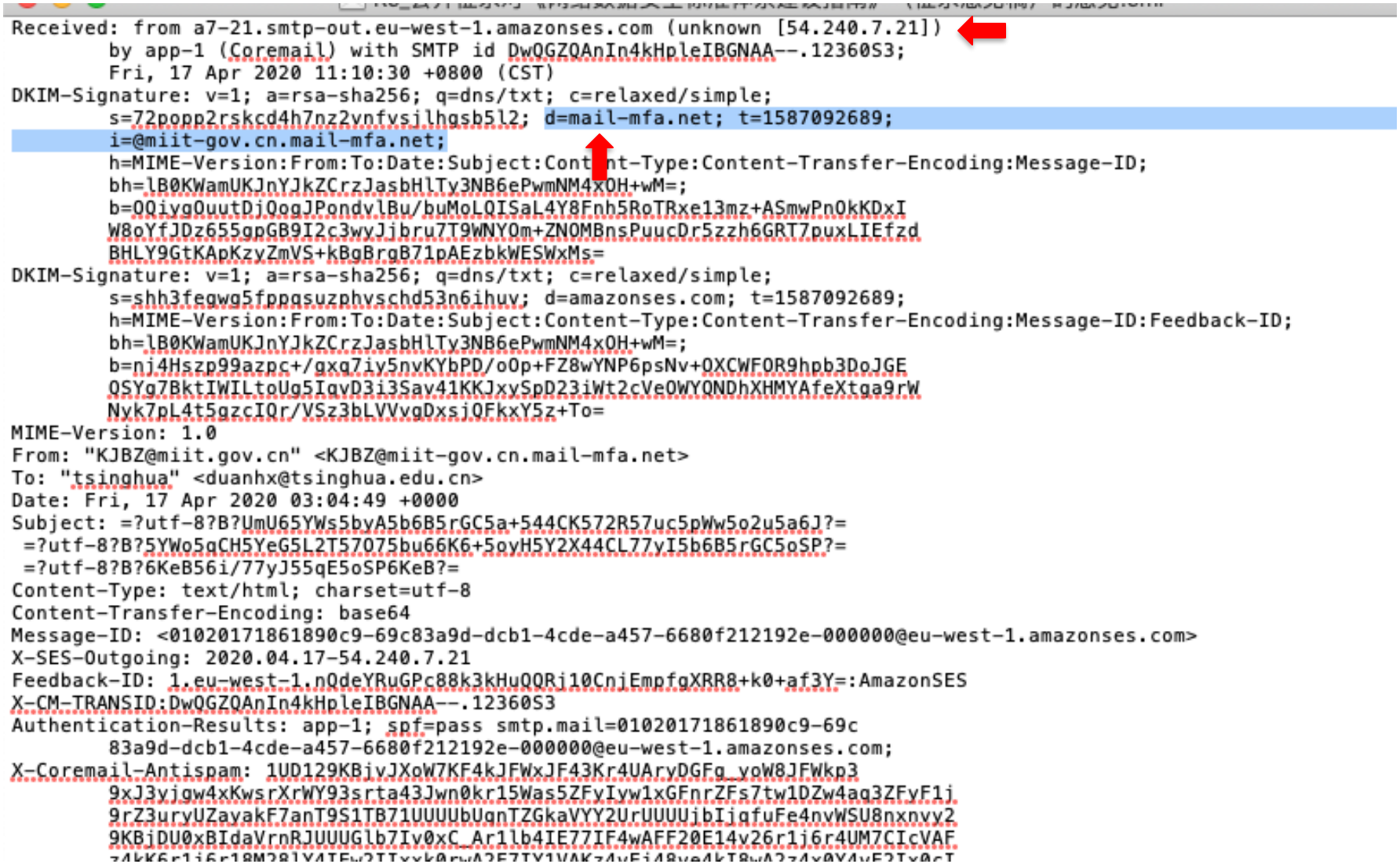
为进一步听取社会各界意见，现予以公示，公示日期截止

这封邮件的意图是什么呢？



http://kjbz.ap1fb.net/images/e038df87/36712/1594/3e3b2a5f/1x1-ffffffff.png

包含DKIM数字签名



```
Received: from a7-21.smtp-out.eu-west-1.amazonses.com (unknown [54.240.7.21])
        by app-1 (Coremail) with SMTP id DwQGZQAnIn4kHpleIBGNAA--.12360S3;
        Fri, 17 Apr 2020 11:10:30 +0800 (CST)
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple;
        s=72popp2rskcd4h7nz2vnfvsjlhgsb5l2; d=mail-mfa.net; t=1587092689;
        i=@miit-gov.cn.mail-mfa.net;
        h=MIME-Version:From:To:Date:Subject:Content-Type:Content-Transfer-Encoding:Message-ID;
        bh=lB0KWamUKJnYJkZCrzJasbHlTy3NB6ePwmNM4xOH+wM=;
        b=QQivgQuutDjOogJPondvlBu/buMoLQISaL4Y8Fnh5RoTRxe13mz+ASmwPnOkKDxI
        W8oYfJDz655gpGB9I2c3wvJjbru7T9WNYOm+ZNOMBnsPuucDr5zzh6GRT7puxLIEfzd
        BHLY9GtKApKzyZmVS+kBgBrgB71pAEzbkWESWxMs=
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple;
        s=shh3fegwg5fppqsuzphvschd53n6ihuv; d=amazonses.com; t=1587092689;
        h=MIME-Version:From:To:Date:Subject:Content-Type:Content-Transfer-Encoding:Message-ID:Feedback-ID;
        bh=lB0KWamUKJnYJkZCrzJasbHlTy3NB6ePwmNM4xOH+wM=;
        b=nj4Hszp99azpc+/gxq7iy5nvKYbPD/oOp+FZ8wYNP6psNv+QXCWFOR9hpb3DoJGE
        QSYg7BktIWILtoUg5IqvD3i3Sav41KKJxySpD23iWt2cVeOWYQNDhXHMYAfeXtga9rW
        Nyk7pL4t5gzcIQr/VSz3bLVVvgDxsjQFkxY5z+To=
MIME-Version: 1.0
From: "KJBZ@miit.gov.cn" <KJBZ@miit-gov.cn.mail-mfa.net>
To: "tsinghua" <duanhx@tsinghua.edu.cn>
Date: Fri, 17 Apr 2020 03:04:49 +0000
Subject: =?utf-8?B?UmU65YWs5byA5b6B5rGC5a+544CK572R57uc5pWw5o2u5a6J?=
 =?utf-8?B?5YWo5qCH5YeG5L2T57O75bu66K6+5oyH5Y2X44CL77yI5b6B5rGC5oSP?=
 =?utf-8?B?6KeB56i/77yJ55qE5oSP6KeB?=
Content-Type: text/html; charset=utf-8
Content-Transfer-Encoding: base64
Message-ID: <01020171861890c9-69c83a9d-dcb1-4cde-a457-6680f212192e-000000@eu-west-1.amazonses.com>
X-SES-Outgoing: 2020.04.17-54.240.7.21
Feedback-ID: 1.eu-west-1.nQdeYRuGPc88k3kHuQQRj10CnjEmpfgXRR8+k0+af3Y=:AmazonSES
X-CM-TRANSID:DwQGZQAnIn4kHpleIBGNAA--.12360S3
Authentication-Results: app-1; spf=pass smtp.mail=01020171861890c9-69c
        83a9d-dcb1-4cde-a457-6680f212192e-000000@eu-west-1.amazonses.com;
X-Coremail-Antispam: 1UD129KBjvJXoW7KF4kJFWxJF43Kr4UAryDGFg_yoW8JFWkp3
        9xJ3yjgw4xKwsrXrWY93srta43Jwn0kr15Was5ZFyIyw1xGFnrZFs7tw1DZw4aq3ZFyF1j
        9rZ3uryUZayakF7anT9S1TB71UUUUbUqnTZGkaVYY2UrUUUUjbIjqfuFe4nvWSU8nxnvy2
        9KBjDU0xBIdaVrnRJUUUGlb7Iv0xC_Ar1lb4IE77IF4wAFF20E14v26r1j6r4UM7CIcVAF
        z4kK6r1j6r18M28lY4IEw2IIxxk0rwA2F7IY1VAKz4vEj48ve4kI8wA2z4x0Y4vE2Ix0cI
```

@段海新 段老师，我们收到一个网络攻击相关的线索

在19号的时候可能有人往你清华的邮箱发过一个攻击邮件

06月30日 10:28

发了三封

都不一样的邮件

贴一下线索截图吧

清华的邮箱的确收到了，但我用的gmail 把这封邮件过滤了

全部已读

所以，我之前没看到这封邮件

全部已读

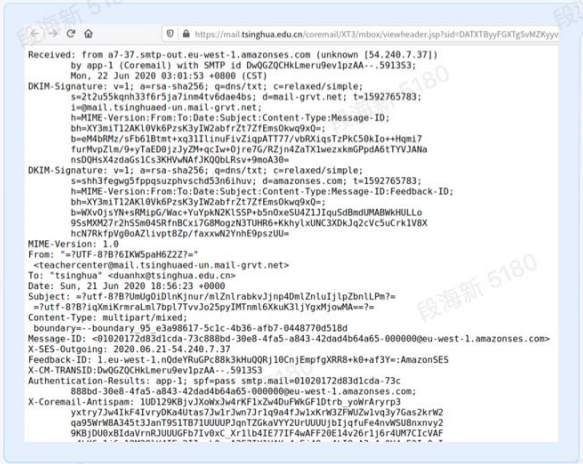
ip

06月30日 12:00

我一会儿从虚拟机里看一下

全部已读

06月30日 12:07



全部已读

2020/6/22 (周一) 2:56

duanhx@tsinghua.edu.cn 代表 肖文静 <teachercenter@mail.tsinghuaed-un.mail-grvt.net>

Re：在线教学优秀教师奖申报截止时间：6月19日中午12:00

收件人 tsinghua

单击此处可下载图片。为了帮助保护您的隐私，Outlook 禁止自动下载该邮件中的某些图片。

Online Teaching Exc...
15 KB

各位老师，

大家好！

在线教学优秀教师奖申报我院材料收集的截止时间是 6 月 19 日 12:00（今天中午），请有意申报的老师直接将申报材料发送本邮箱。

欢迎老师们积极申报！

-----原始邮件-----

发件人:"肖文静"〈teachercenter@mail.tsinghua.edu.cn〉


奖申报我院材料收集的截止时间是 6
报！

〈teachercenter@mail.tsinghua.e
06-17 19:10:03（星期三）
tsinghua
添加
联系人
日历
安排会议
发送电子邮件
duanhx@tsinghua.edu.cn
报材

某些部门在追踪这个 APT 组织，监控了这个肖文静邮箱，那个邮箱是伪造的

你可以问问那个人是不是被攻击过

施叶林

按理说被攻击的概率很大

06月30日 12:19

肖文静 <teachercenter@mail.tsinghuaed-un.mail-grvt.net> 这个邮箱后缀是印度攻击者注册的

有的邮件客户端只显示邮件地址的一部分

06月30日 12:27

还给您发了两封邮件，邮箱后缀是 mail-mfa.net

应该给清华好多人发了

访问记录有很多不同的清华 ip

来自mail-mfa.net 的有两封

Re：在线教学优秀教师奖申报截止时间：6月19日中午12:00 发起会议

发件人： 肖文静 <teac...@mail.tsinghuaed-un.mail-grvt.net>

(由 01020172d83d1cda-73c888bd-30e8-4fa5-a843-42dad4b64a65-000000@eu-west-1.amazonses.com 代发)

时 间： 2020年06月22日 02:56:23 (星期一)

收件人： tsinghua <duanhx@tsinghua.edu.cn>

： 1 个 (W Online Teaching Excellence.docx) 查看附件

各位老师，

大家好！

在线教学优秀教师奖申报我院材料收集的截止时间是6月19日12:00（今天中午），请有意申报的

欢迎老师们积极申报！

-----原始邮件-----
发件人:"肖文静" <teachercenter@mail.tsinghua.edu.cn>
发送时间:2020-06-17 19:10:03 (星期三)

主题: 在线教学优秀教师奖申报

```
Received: from a7-37.smtp-out.eu-west-1.amazonses.com (unknown [54.240.7.37])
        by app-1 (Coremail) with SMTP id DwQGZQCHkLmeru9ev1pzAA--.5913S3;
        Mon, 22 Jun 2020 03:01:53 +0800 (CST)
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple;
        s=2t2u55kqnh33f6r5ja7inm4tv6dae4bs; d=mail-grvt.net; t=1592765783;
        i=@mail.tsinghuaed-un.mail-grvt.net;
        h=MIME-Version:From:To:Date:Subject:Content-Type:Message-ID;
        bh=XY3miT12AKl0Vk6PzsK3yIW2abfrZt7ZfEmsOkwq9xQ=;
        b=eM4bRMz/sFb61Btmt+xq31IlinuFivZiqpATT77/vbRXiqsTzPkC50kIo++Hqmi7
        furMvpZlm/9+yTaED0jzJyZM+qcIw+Ojre7G/RZjn4ZaTX1wezxkmGPpdA6tTYVJANa
        nsDQHsX4zdaGs1Cs3KHVwNAfJKQQbLRsv+9moA30=
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/simple;
        s=shh3fegwg5fppqsuzphvschd53n6ihuv; d=amazonses.com; t=1592765783;
        h=MIME-Version:From:To:Date:Subject:Content-Type:Message-ID:Feedback-ID;
        bh=XY3miT12AKl0Vk6PzsK3yIW2abfrZt7ZfEmsOkwq9xQ=;
        b=WXvOjsYN+sRMipG/Wac+YuYpkN2KlSSP+b5nOxeSU4Z1JIquSdBmdUMABWkHULLo
        9SsMXM27r2hSSm04SRfnBCxi7G8MogzN3TUHR6+KkhylxUNC3XDkJq2cVc5uCrk1V8X
        hcN7RkfpVg0oAZlivpt8Zp/faxxwN2YnhE9pszUU=
MIME-Version: 1.0
From: "=?UTF-8?B?6IKW5paH6Z2Z?="
 <teachercenter@mail.tsinghuaed-un.mail-grvt.net>
To: "tsinghua" <duanhx@tsinghua.edu.cn>
Date: Sun, 21 Jun 2020 18:56:23 +0000
Subject: =?utf-8?B?UmUgOiDlnKjnur/mlZnlrabkvJjnp4DmlZnluIjlpZbnlLPm?=
 =?utf-8?B?iqXmiKrmraLml7bpl7TvvJo25pyIMTnml6XkuK3ljYgxMjowMA==?=
Content-Type: multipart/mixed;
 boundary=--boundary_95_e3a98617-5c1c-4b36-afb7-0448770d518d
Message-ID: <01020172d83d1cda-73c888bd-30e8-4fa5-a843-42dad4b64a65-000000@eu-west-1.amazonses.com>
X-SES-Outgoing: 2020.06.21-54.240.7.37
Feedback-ID: 1.eu-west-1.nQdeYRuGPc88k3kHuQQRj10CnjEmpfgXRR8+k0+af3Y=:AmazonSES
X-CM-TRANSID:DwQGZQCHkLmeru9ev1pzAA--.5913S3
Authentication-Results: app-1; spf=pass smtp.mail=01020172d83d1cda-73c
        888bd-30e8-4fa5-a843-42dad4b64a65-000000@eu-west-1.amazonses.com;
X-Coremail-Antispam: 1UD129KBjvJXoWxJw4rKF1xZw4DuFWkGF1Dtrb_yoWrAryrp3
        yxtry7Jw4IkF4IvryDKa4Utas7Jw1rJwn7Jr1q9a4fJw1xKrW3ZFWUZw1vq3y7Gas2krW2
        qa95WrW8A345t3JanT9S1TB71UUUUPJqnTZGkaVYY2UrUUUUjbIjqfuFe4nvWSU8nxnvy2
        9KBjDU0xBIdaVrnRJUUUGFb7Iv0xC_Xr1lb4IE77IF4wAFF20E14v26r1j6r4UM7CIcVAF
```

duanhx@tsinghua.edu.cn整改通知 Inbox ×

thucio@tsinghua.edu.cn <thucio@tsinghua.edu.c… Fri, Sep 4, 4:34 PM

to duanhx

段海新 老师： 你好

接到教育部通知您的邮箱有安全问题详见附件。请于9月7日12点前网站检查和整改工作，并按整改通知下面内容的要求写一份整改报告。

2020-09-04
清华大学信息化工作办公室

thucio@tsinghua.edu.cn

电话：010-62780257
地址：清华大学李兆基A362
...

[Message clipped] View entire message

清华大学

重要威胁通知报告

1. 网站相关信息

网站名称： **清华大学所属邮箱(事件编号：EVENT-202007081559)**

威胁名称：网络攻击

威胁邮箱：duanhx@tsinghua.edu.cn

2. 威胁验证截图

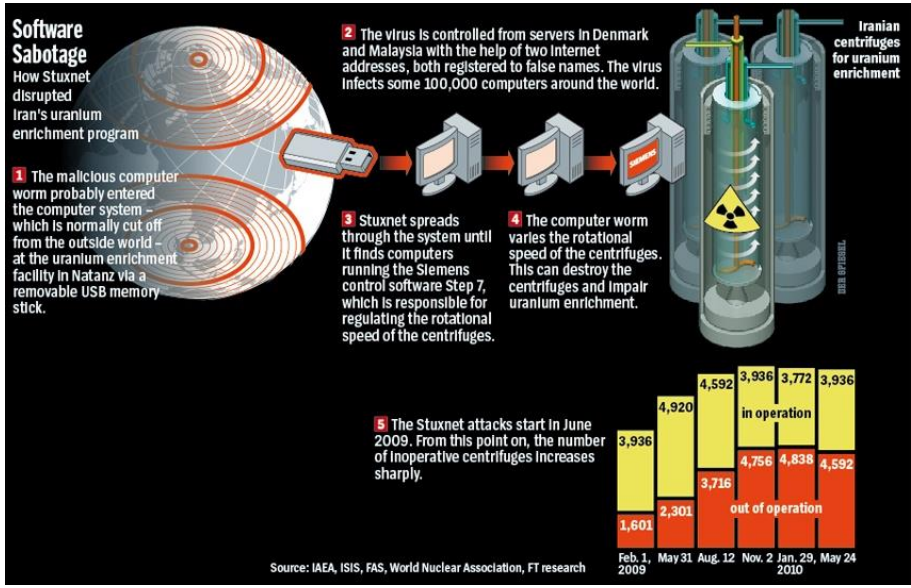
近期监测发现，清华大学所属邮箱duanhx@tsinghua.edu.cn遭钓鱼邮件攻击,邮件主题为“Re: 在线教学优秀教师奖申报截止时间：6月19日上午12:00”

3. 威胁修复建议

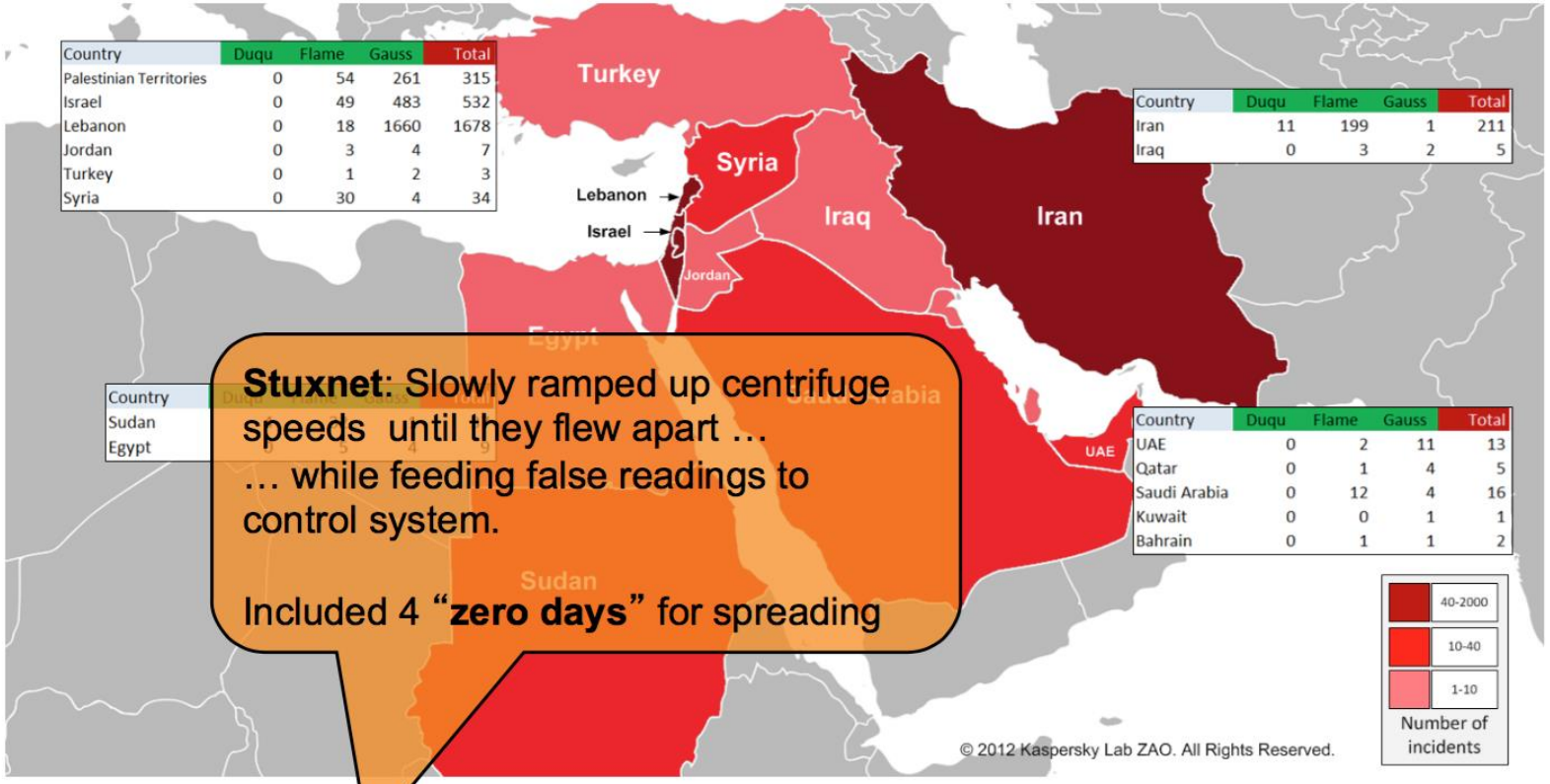
按网信办要求，在本平台反馈事件处置详情时应附上事件处置过程附件！附件内容包括事件核验情况、排查过程，损失与危害情况、协调处置过程、涉事系统运营单位和整改情况，如有下一步防护计划，也请说明。如有疑问，可致电010-82991537或者010-55635445

Cyber Warefare: Stuxnet 2010

- Attacks industrial control systems likely an Iranian uranium enrichment facility
- Modifies and hides code on Siemens PLCs connected to frequency converters
- Contains 7 methods to propagate, 4 zero day exploits, 1 known exploit, 3 rootkits, 2 unauthorized certificates, 2 Siemens security issues.
- 3 versions, June 2009, March 2010, April 2010



https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1493844778.pdf



Country	Duqu	Flame	Gauss	Total
Palestinian Territories	0	54	261	315
Israel	0	49	483	532
Lebanon	0	18	1660	1678
Jordan	0	3	4	7
Turkey	0	1	2	3
Syria	0	30	4	34

Country	Duqu	Flame	Gauss	Total
Iran	11	199	1	211
Iraq	0	3	2	5

Country	Duqu	Flame	Gauss	Total
UAE	0	2	11	13
Qatar	0	1	4	5
Saudi Arabia	0	12	4	16
Kuwait	0	0	1	1
Bahrain	0	1	1	2

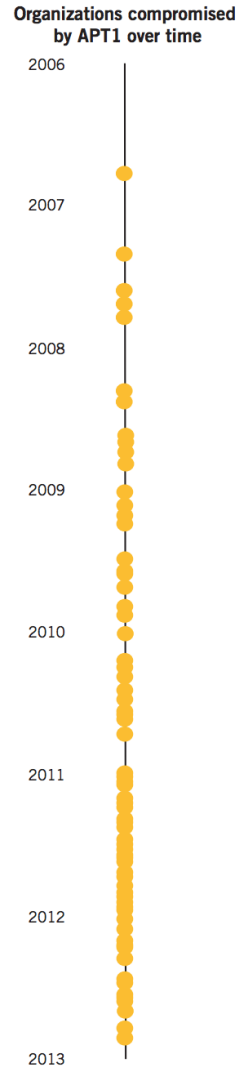
Country
Sudan
Egypt

Stuxnet

Flame

Gauss

APT1: Exposing One of China's Cyber Espionage Units



APT1: YEARS OF ESPIONAGE

Our evidence indicates that APT1 has been stealing hundreds of terabytes of data from at least 141 organizations across a diverse set of industries beginning as early as 2006. Remarkably, we have witnessed APT1 target dozens of organizations simultaneously. Once the group establishes access to a victim's network, they continue to access it periodically over several months or years to steal large volumes of valuable intellectual property, including technology blueprints, proprietary manufacturing processes, test results, business plans, pricing documents, partnership agreements, emails and contact lists from victim organizations' leadership. We believe that the extensive activity we have directly observed represents only a small fraction of the cyber espionage that APT1 has committed.

APT1 Puts the "Persistent" in APT

Since 2006 we have seen APT1 relentlessly expand its access to new victims. Figure 10 shows the timeline of the 141 compromises we are aware of; each marker in the figure represents a separate victim and indicates the earliest *confirmed* date of APT1 activity in that organization's network.[26]

With the ephemeral nature of electronic evidence, many of the dates of earliest known APT1 activity shown here underestimate the duration of APT1's presence in the network.

FIGURE 10: Timeline showing dates of earliest known APT1 activity in the networks of the 141 organizations in which Mandiant has observed APT1 conducting cyber espionage.

[26] Figure 10 shows that we have seen APT1 compromise an increasing number of organizations each year, which may reflect an increase in APT1's activity. However, this increase may also simply reflect Mandiant's expanding visibility into APT1's activities as the company has grown and victims' awareness of cyber espionage activity in their networks has improved.

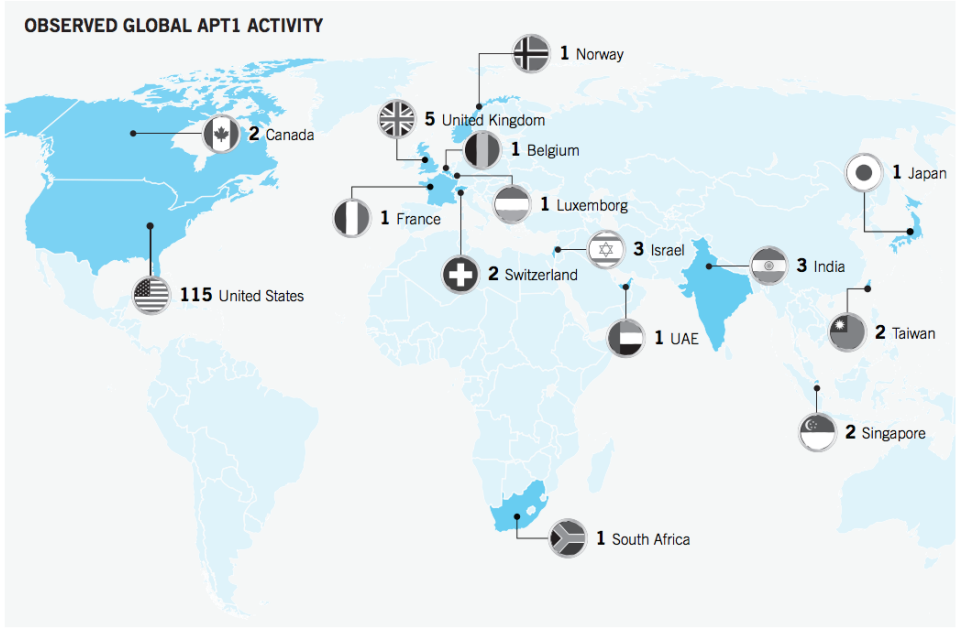


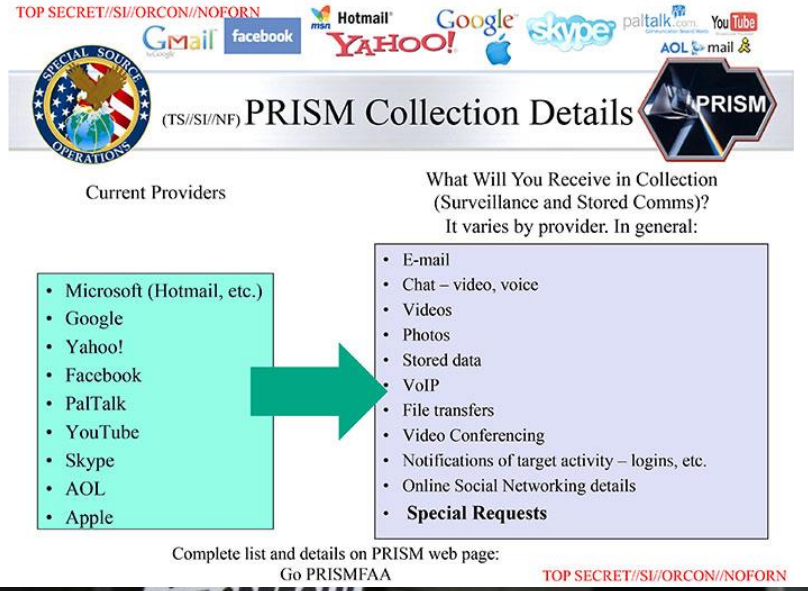
FIGURE 11: Geographic location of APT1's victims. In the case of victims with a multinational presence, the location shown reflects either the branch of the organization that APT1 compromised (when known), or else is the location of the organization's headquarters.

APT1 has demonstrated the capability and intent to steal from dozens of organizations across a wide range of industries virtually simultaneously. Figure 12 provides a view of the earliest known date of APT1 activity against all of the 141 victims we identified, organized by the 20 major industries they represent. The results suggest that APT1's mission is extremely broad; the group does not target industries systematically but more likely steals from an enormous range of industries on a continuous basis. Since the organizations included in the figure represent only the fraction of APT1 victims that we confirmed directly, the range of industries that APT1 targets may be even broader than our findings suggest.

Further, the scope of APT1's parallel activities implies that the group has significant personnel and technical resources at its disposal. In the first month of 2011, for example, Figure 12 shows that APT1 successfully compromised 17 new victims operating in 10 different industries. Since we have seen that the group remains active in each victim's network for an average of nearly a year after the initial date of compromise, we infer that APT1 committed these 17 new breaches while simultaneously maintaining access to and continuing to steal data from a number of previously compromised victims.

https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

PRISM leaked by Snowden, 2013



China

EXCLUSIVE: NSA targeted China's Tsinghua University in extensive hacking attacks, says Snowden

Tsinghua University, widely regarded as the mainland's top education and research institute, was the target of extensive hacking by US spies this year

Lana Lam

Published: 11:24pm, 22 Jun, 2013

TOP PICKS

This Week in Asia

If the US and China go to war, whose side is Southeast Asia on?

21 Sep 2020

This Week in Asia

Why Russia's getting involved in the China-India border dispute

19 Sep 2020

News

Coronavirus is beat

QUANTUM Capabilities – NSA

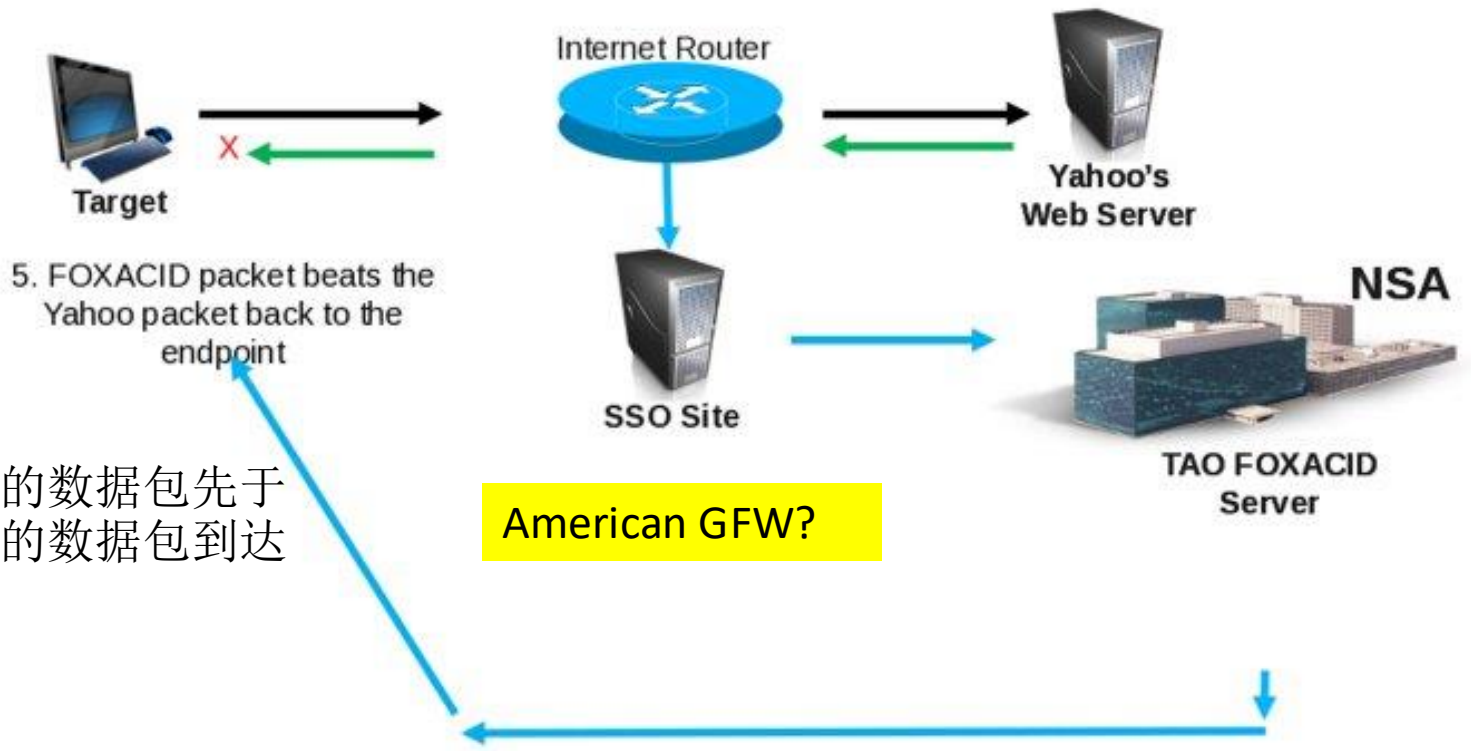
(TS//SI//REL) NSA QUANTUM has the *greatest* success against <yahoo>, <facebook>, and Static IP Addresses. New QUANTUM realms are often changing, so check the GO QUANTUM wiki page or the QUANTUM SpySpace page to get more up-to-date news.

NSA QUANTUM is capable of targeting the following realms:

- IPv4_public
- alibabaForumUser
- doubleclickID
- emailAddr
- rocketmail
- hi5Uid
- hotmailCID
- linkedin
- mail
- mailruMrcu
- msnMailToken64
- mailruMrcu
- msnMailToken64
- qq
- facebook
- simbarUuid
- twitter
- yahoo
- yahooBcookie
- ymail
- youTube
- WatcherID

What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works



伪造的数据包先于
合法的数据包到达

American GFW?

Internet Engineering Task Force (IETF)
Request for Comments: 7258
BCP: 188
Category: Best Current Practice
ISSN: 2070-1721

S. Farrell
Trinity College Dublin
H. Tschofenig
ARM Ltd.

May 2014

Pervasive Monitoring Is an Attack

Abstract

Pervasive monitoring is a technical attack that should be mitigated in the design of IETF protocols, where possible.

Threat: Big Brother

edition.cnn.com/2013/03/16/opinion/schneier-internet-surveillance

STORY HIGHLIGHTS

- Bruce Schneier: Whether we like it or not, we're being tracked all the time on the Internet
- Schneier: Our surveillance state is efficient beyond the wildest dreams of George Orwell
- He says governments and corporations are working together to keep things that way
- Schneier: Slap-on-the-wrist fines notwithstanding, no one is agitating for better privacy laws

Editor's note: *Bruce Schneier is a security technologist and author of "Liars and Outliers: Enabling the Trust Society Needs to Survive."*

(CNN) -- I'm going to start with three data points.

One: Some of the Chinese military hackers who were implicated in a broad set of attacks against the U.S. government and corporations were identified because they accessed Facebook from the same network infrastructure they used to carry out their attacks.

Two: Hector Monsegur, one of the leaders of the LulzSac hacker movement, was identified and arrested last year by the FBI. Although he practiced good computer security and used an anonymous relay service to protect his identity, he slipped up.

Bruce Schneier

And three: Paula Broadwell,who had an affair with CIA director David Petraeus, similarly took extensive precautions to hide her identity. She never logged in to her anonymous e-mail service from her home network. Instead, she used hotel and other public networks when she e-mailed him. The FBI correlated hotel registration data from several different hotels -- and hers was the common name.

The Internet is a surveillance state. Whether we admit it to ourselves or not, and whether we like it or not, we're being tracked all the time. Google tracks us, both on its pages and on other pages

June 8, 2013 – Updated 1736 GMT (0136 HKT)

Van Jones says governme surveillance programs are symptoms of broader char that will shake up our government and society fo many decades to come.

Privacy is not dead

June 8, 2013 – Updated 1828 GMT (0228 HKT)

Jack Cheng says young people are already sharing everything anyway, so doe privacy still matter?

Holocaust artifacts bear witness

June 8, 2013 – Updated 1453 GMT (2253 HKT)

Suzy Snyder: The U.S. Holocaust Memorial Museu collecting artifacts that tell t story of Nazi Germany.

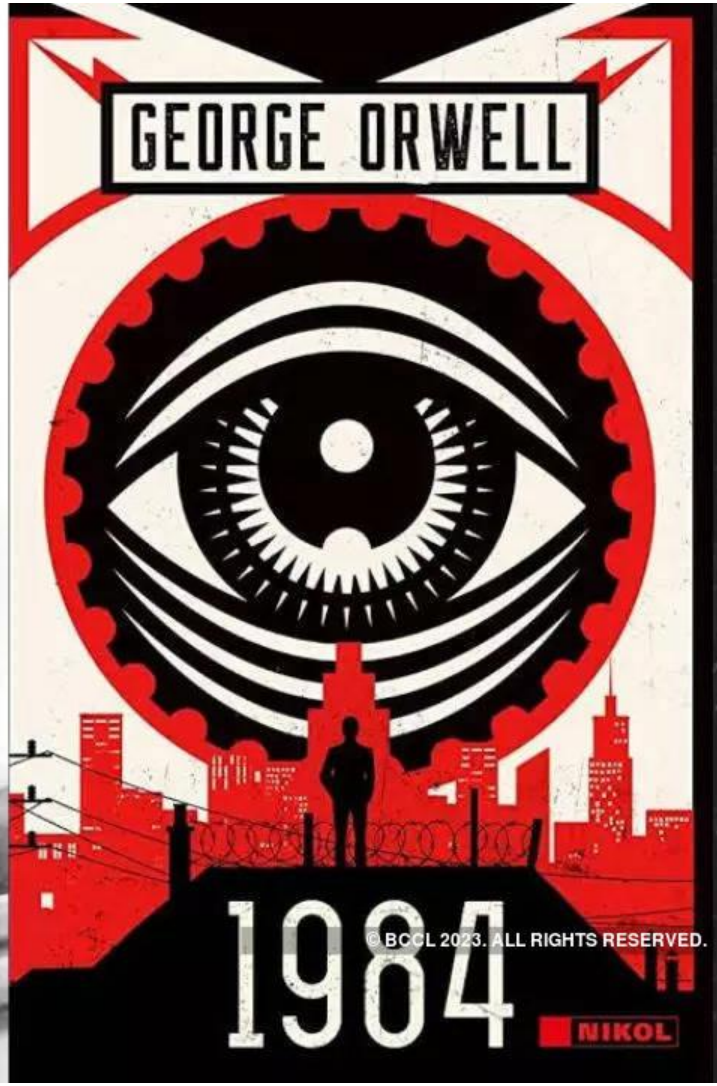
Thank you, Michael Douglas

June 7, 2013 – Updated 1913 GMT (0313 HKT)

Dean Obeidallah, John Avl and Margaret Hoover disc IRS's lavish spending, hec and Michael Douglas.

This is what a surveillance state looks like, and it's efficient beyond the wildest dreams of George Orwell.

《1984》， George Orwell

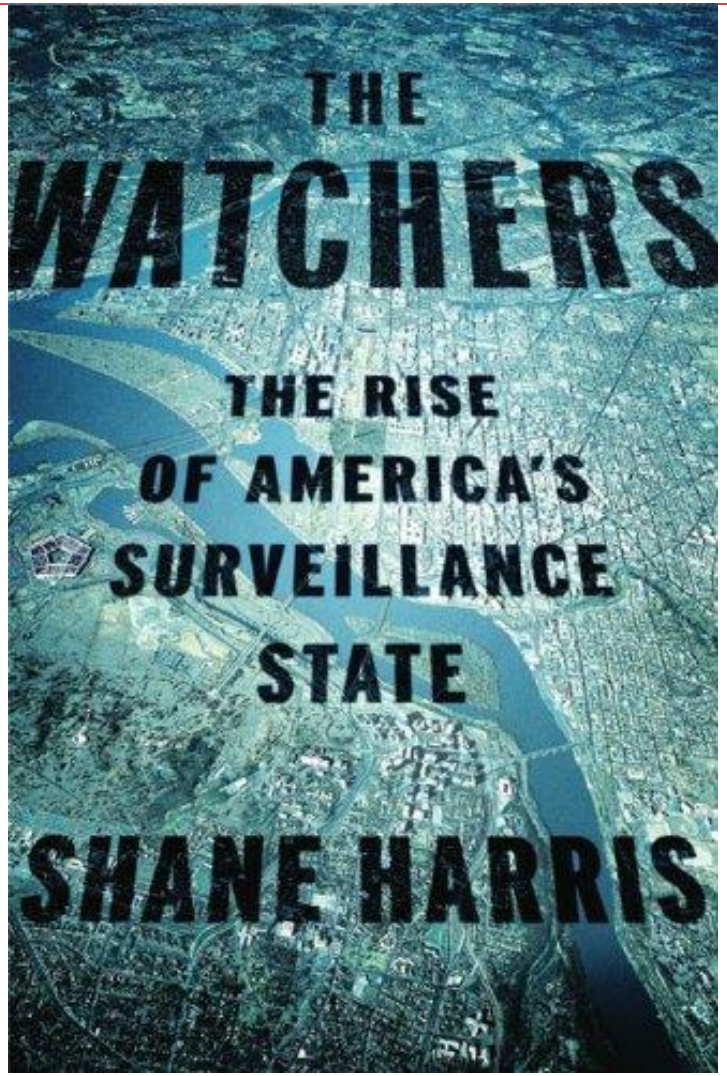


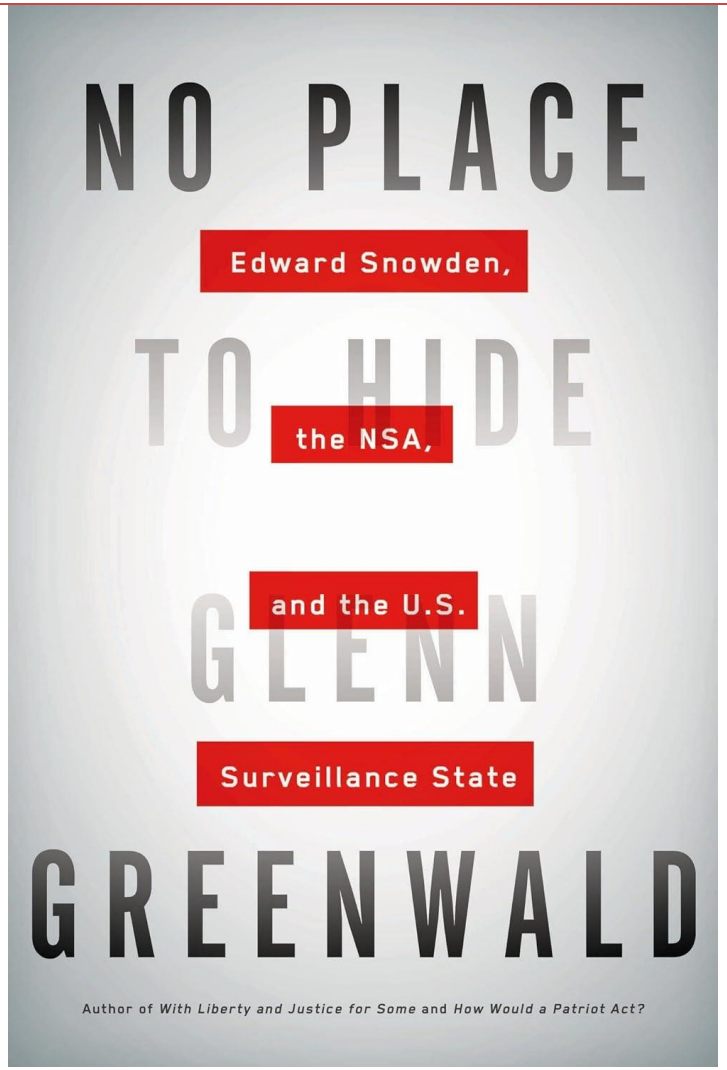
Surveillance State

Surveillance

Surveillance

USA, the Surveillance State





总结：需要理解的概念

- 风险评估模型：资产、漏洞、敌手
- 三个不同阶段的漏洞
- 高级持续威胁（APT）
- 安全的目标：CIA
- 安全是攻防之间持续的对抗