防病毒软件还是防病毒服务?
ARP欺骗木马治理与对策

商尔从　　SYSU-CSIRT

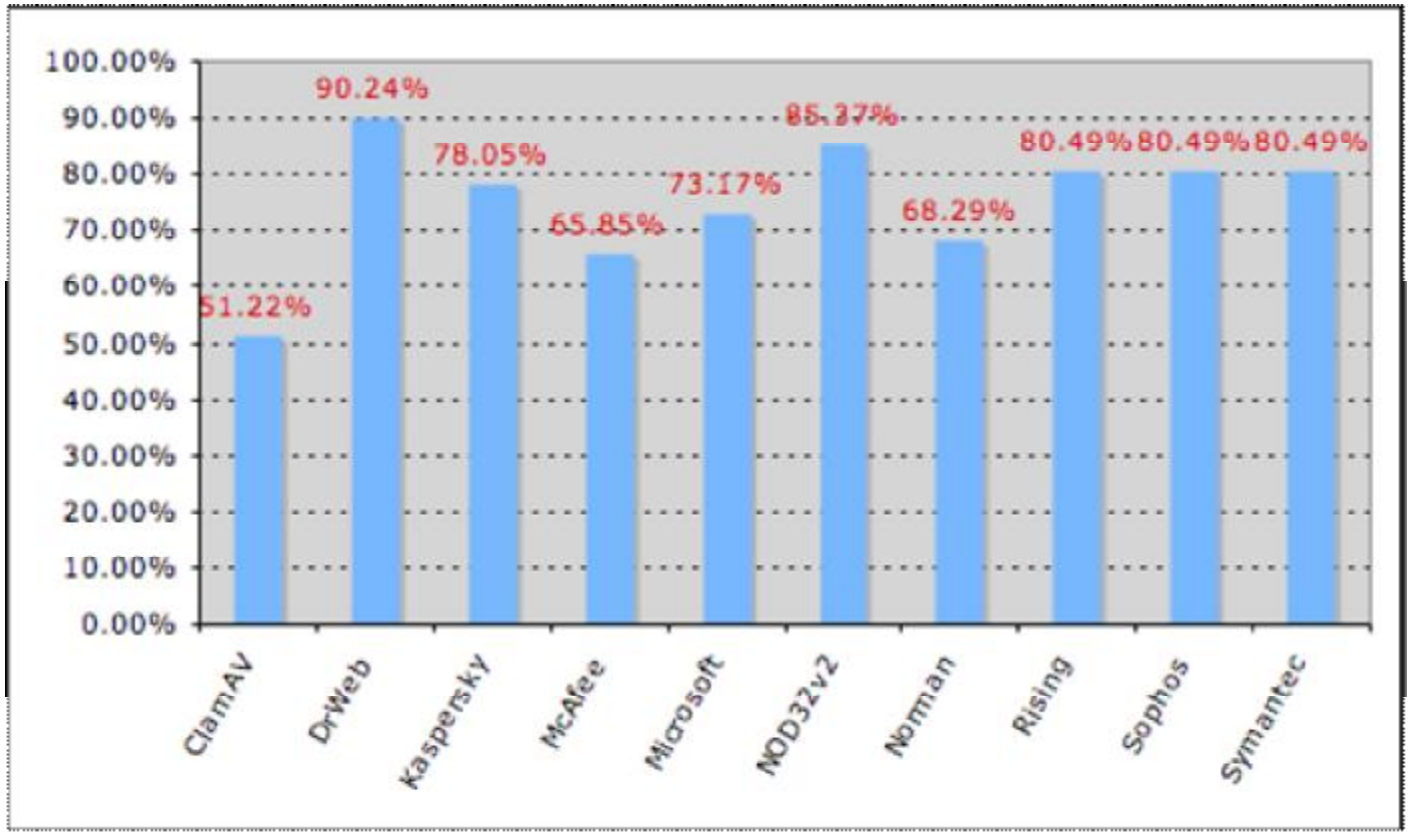
中山大学信息与网络中心

议题

- 防病毒软件还是防病毒服务?
- ARP欺骗木马治理与对策

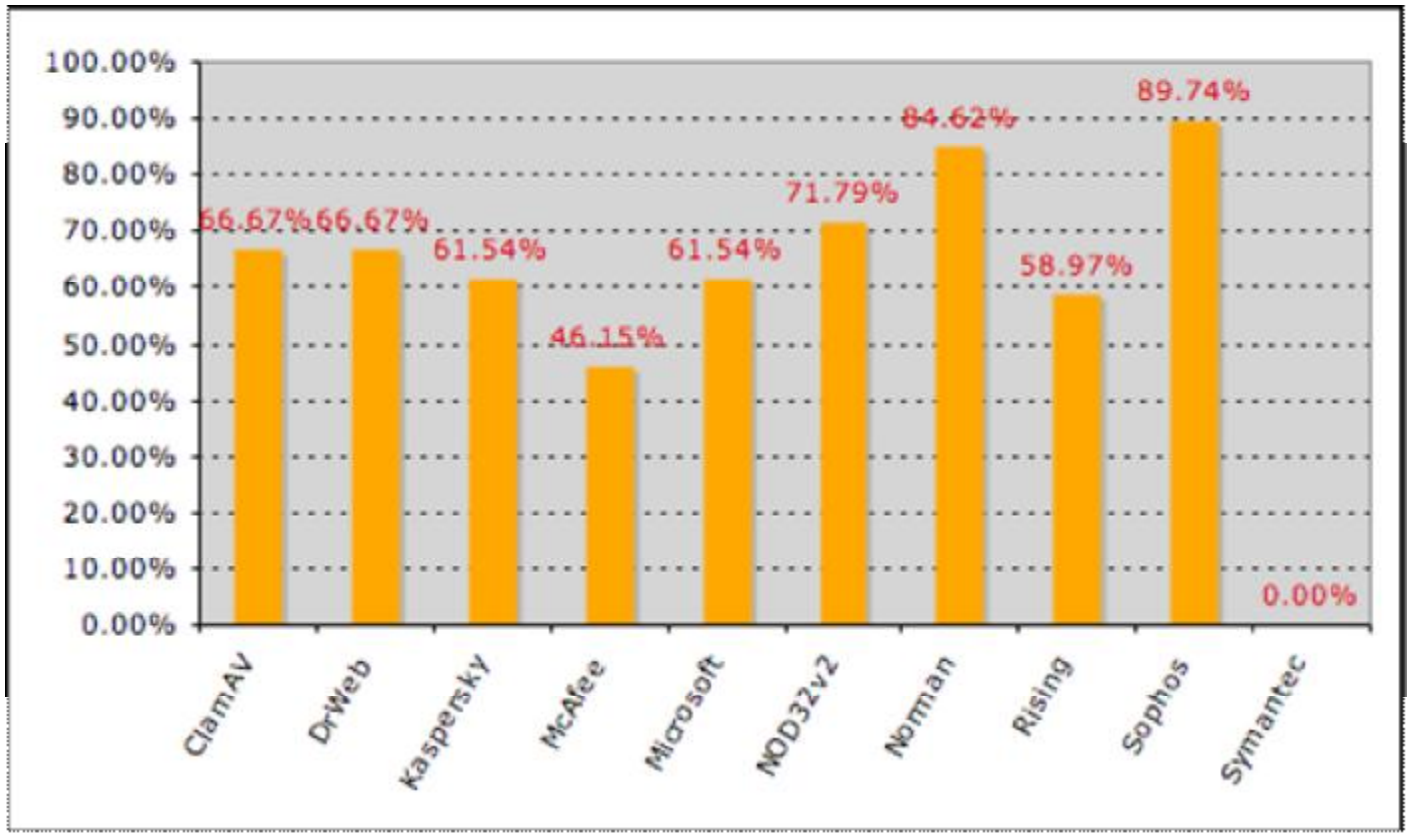
防病毒软件还是防病毒服务?

07’9-10提交VirusTotal 41个样本首次提交检出率



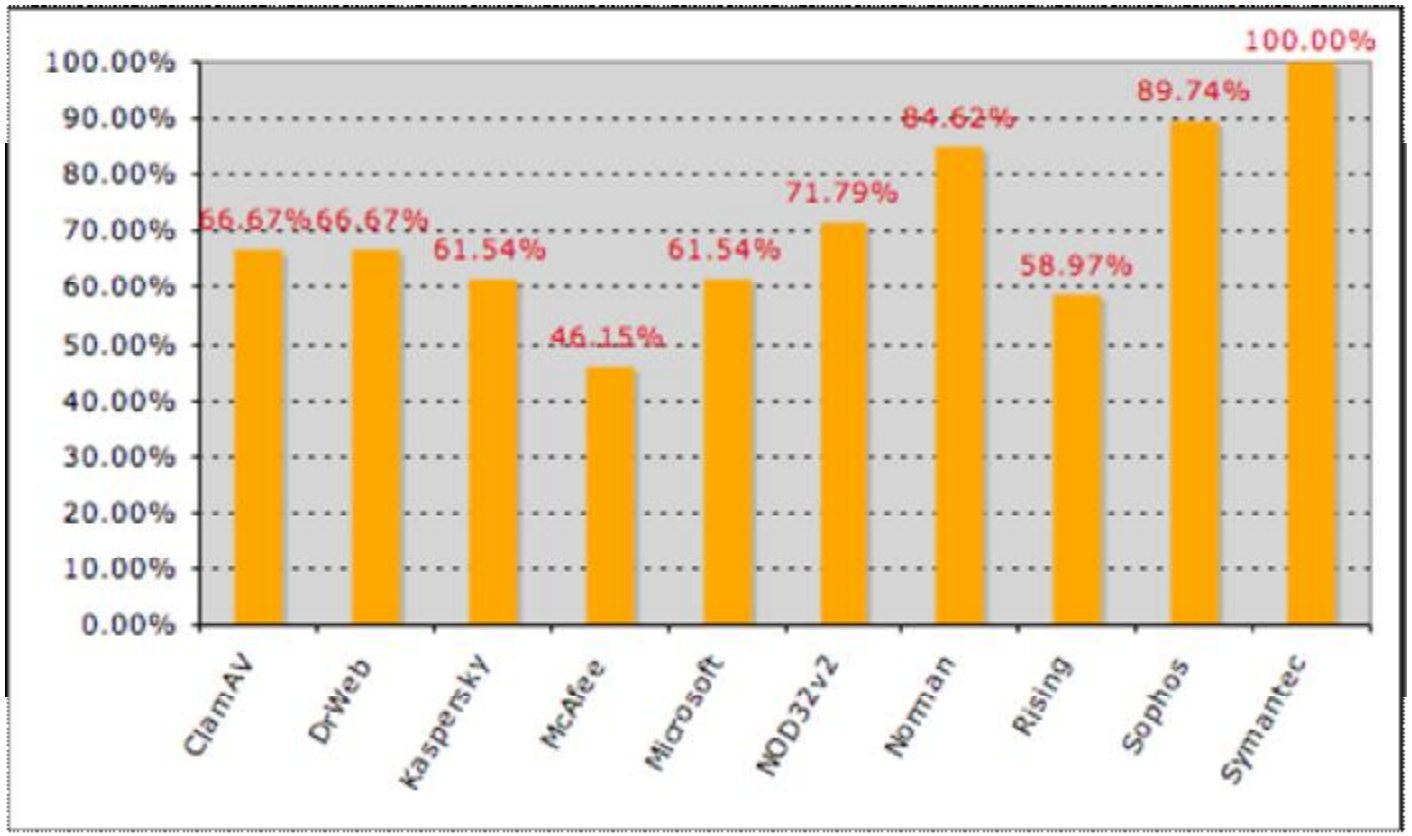
2007年9月-10月收集的41个病毒样本首次提交检出率统计

08’1-3 Symantec无法检出的样本首次提交VirusTotal对比检出率(1)



2008年1月-3月收集的39个样本Symantec首次无法检出

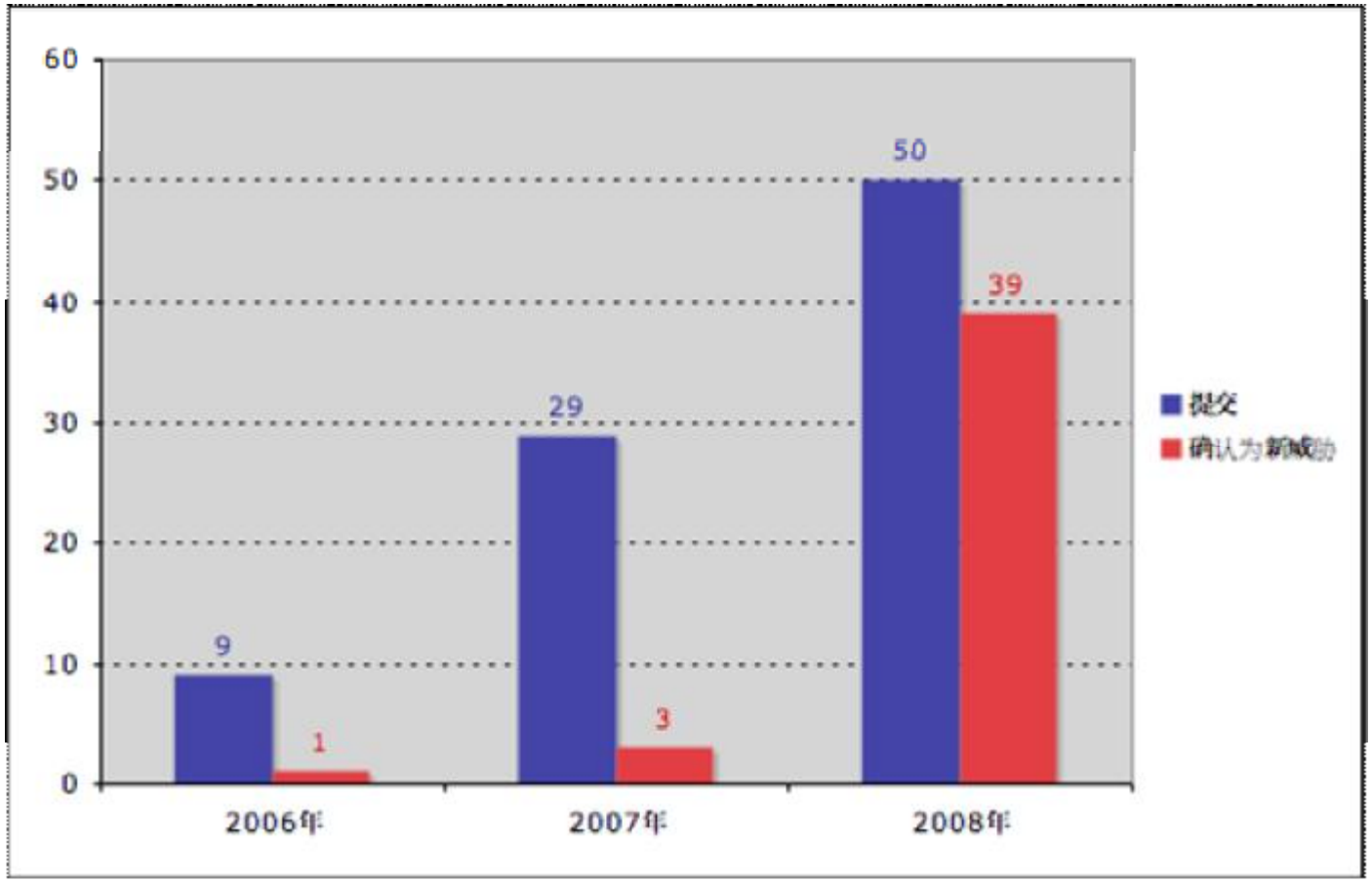
08’1-3 Symantec无法检出的样本
Symantec修订病毒定义检出率会变化



2008年1-3月收集的39个样本Symantec增加到病毒定义中

Symantec修订病毒定义后检出率会发生变化。

SYSU-CSIRT提交样本Symantec新增补的定义



VirusTotal有助样本提交及提高样本提交的准确性

专业的防病毒服务支持

- 防病毒软件产品 (仅是防病毒服务中的一部分)
- CSIRT现场事件响应服务
- 帮助台支持/知识库
- 风险分析威胁管理
- 披露与公告
- 教育与培训
- 安全意识

正确认识防病毒软件

- 防病毒软件不是万能的
- 防病毒软件需要配合辅助工具
  - 防御工具
  - 清理工具
  - 修复工具
- “主动防御”尚待成熟

正确使用防病毒软件

- 高校信息安全部门提供一线服务与支持
- 要与防病毒软件厂家共享信息
- 要对防病毒软件产品作出“贡献”
- 善用防病毒软件厂家的二线支持服务
- 善用防病毒软件病毒数据库进行风险评估
  - 广泛性
  - 危害性
  - 分发能力

提高意识取得信任是关键

- 提升意识和信任需要精密策划与长时间的积累
- 拒绝求助将会丧失信任
- 错误的安全意识比无安全意识更糟
- 盗版防病毒软件=假冒伪劣安全产品

安全意识与教育(1)

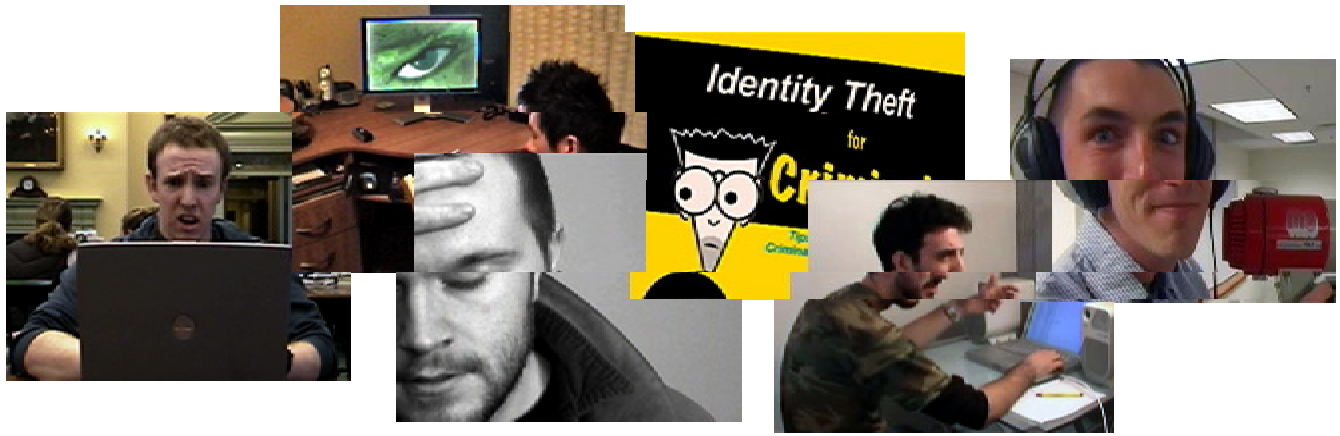

Importance of information security awareness
Approaches to raise awareness
Approaches to raise awareness
Retailer – fitting in with the culture
Information security awareness initiatives:
Current practice and the measurement of success
July 2007
enisa
European Network and Information Security Agency

ENISA 2007年工作纲要中提升意识和建立信任的地位

资料来源: ENISA http://www.enisa.europa.eu/

安全意识与教育(2)

2006 - 2007 Computer Security Awareness Video Contest



安全意识与教育(3)


資訊保安管理四重奏
保護你的電腦資料
如何保護你的電腦資料？
保護你的電腦資料
Protect Your
Computer Data
警告 WARNING
www.infosec.gov.hk

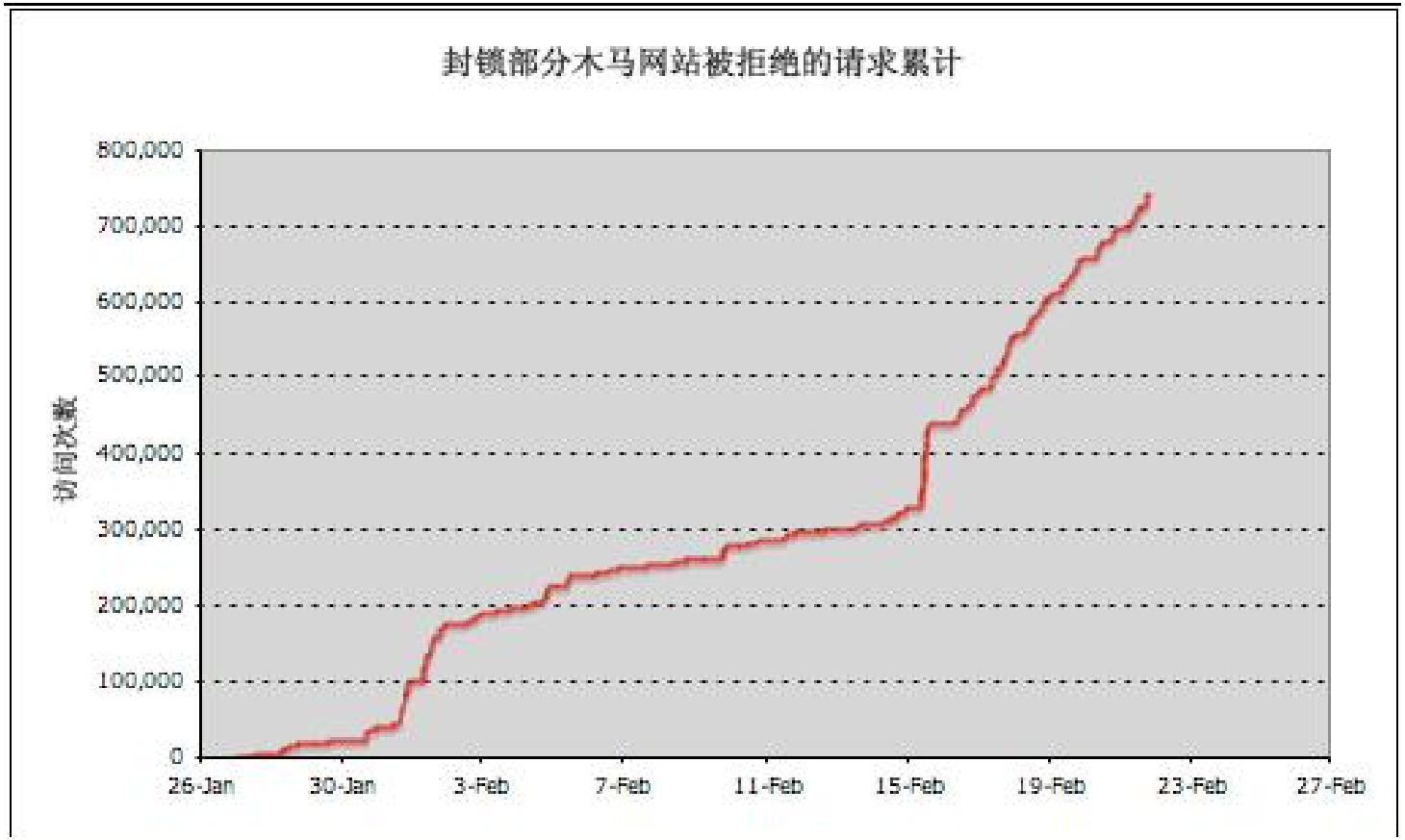
ARP欺骗木马治理与对策

对《治理ARP欺骗围堵下载器和安装器木马》
的补充

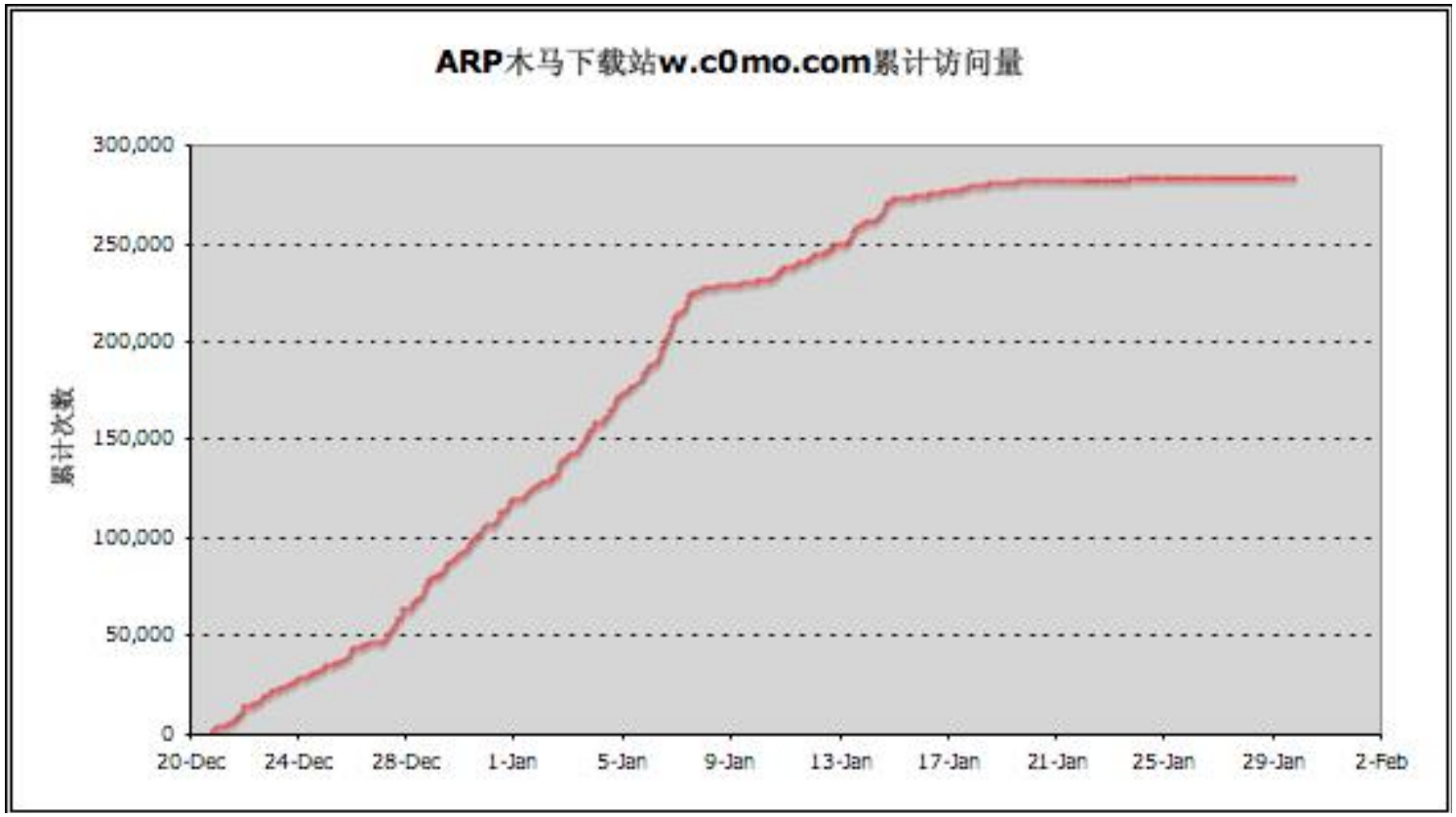
ARP欺骗的目的和类型

- ARP欺骗的目的是信息犯罪者为截获盗取有价值的信息资产，并将盗取的信息资产用于黑市交易，谋取暴利。
- ARP欺骗的类型
  - 入侵型：信息犯罪者入侵有漏洞的服务器，使用专用黑客工具进行ARP欺骗劫持通讯，并在HTTP通讯中插入恶意代码，导致访问同网段的服务器时感染木马(一般为下载器或者安装器木马)，是信息犯罪者首次分发木马的重要机制。
  - 木马型：普通计算机感染了ARP欺骗木马后劫持同一网段通讯的重要手段，以收集用户的有价值的信息资产。

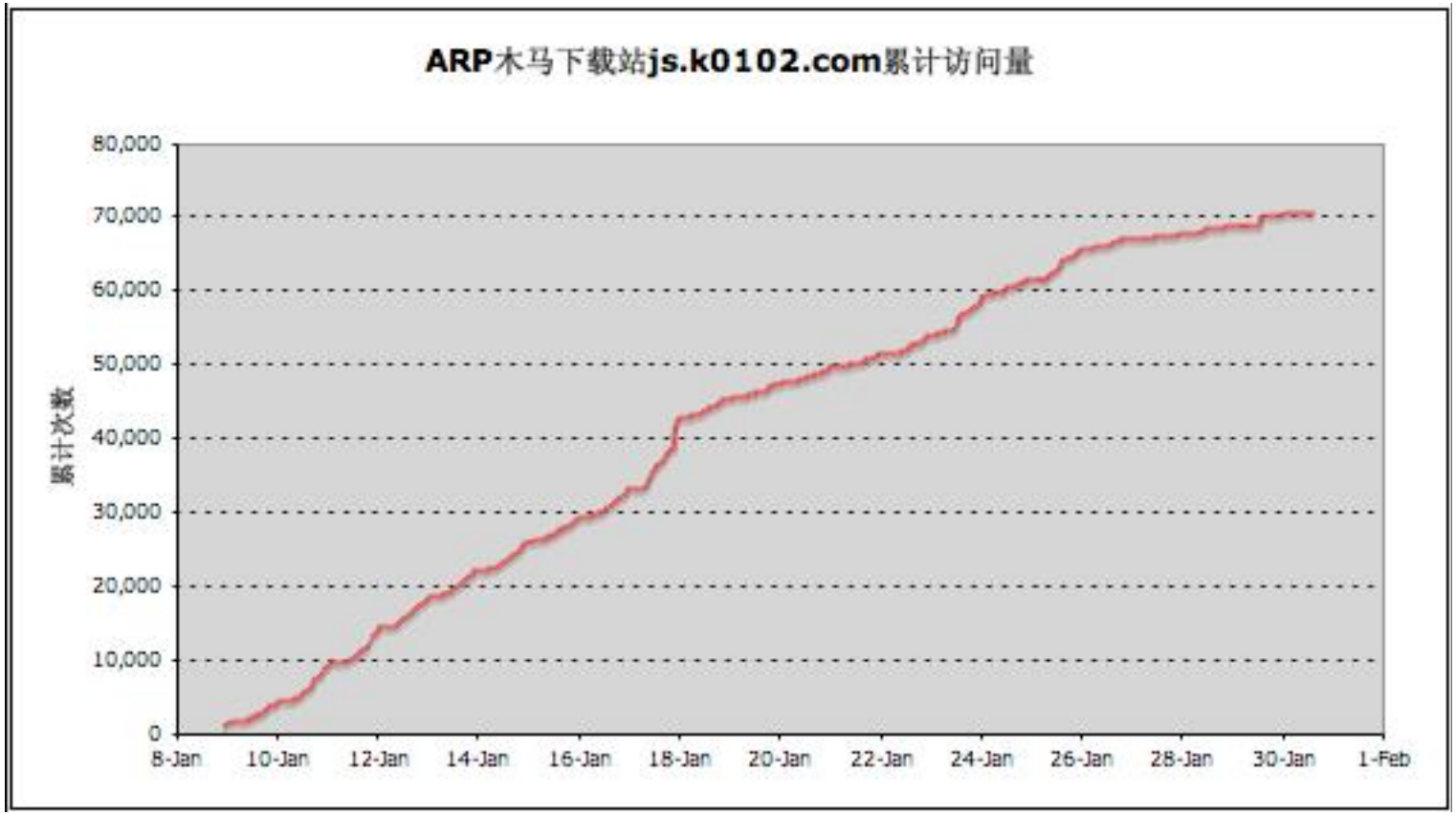
封锁木马网站的有效性


封锁部分木马网站被拒绝的请求累计
访问次数
800,000
700,000
600,000
500,000
400,000
300,000
200,000
100,000
0
26-Jan
30-Jan
3-Feb
7-Feb
11-Feb
15-Feb
19-Feb
23-Feb
27-Feb

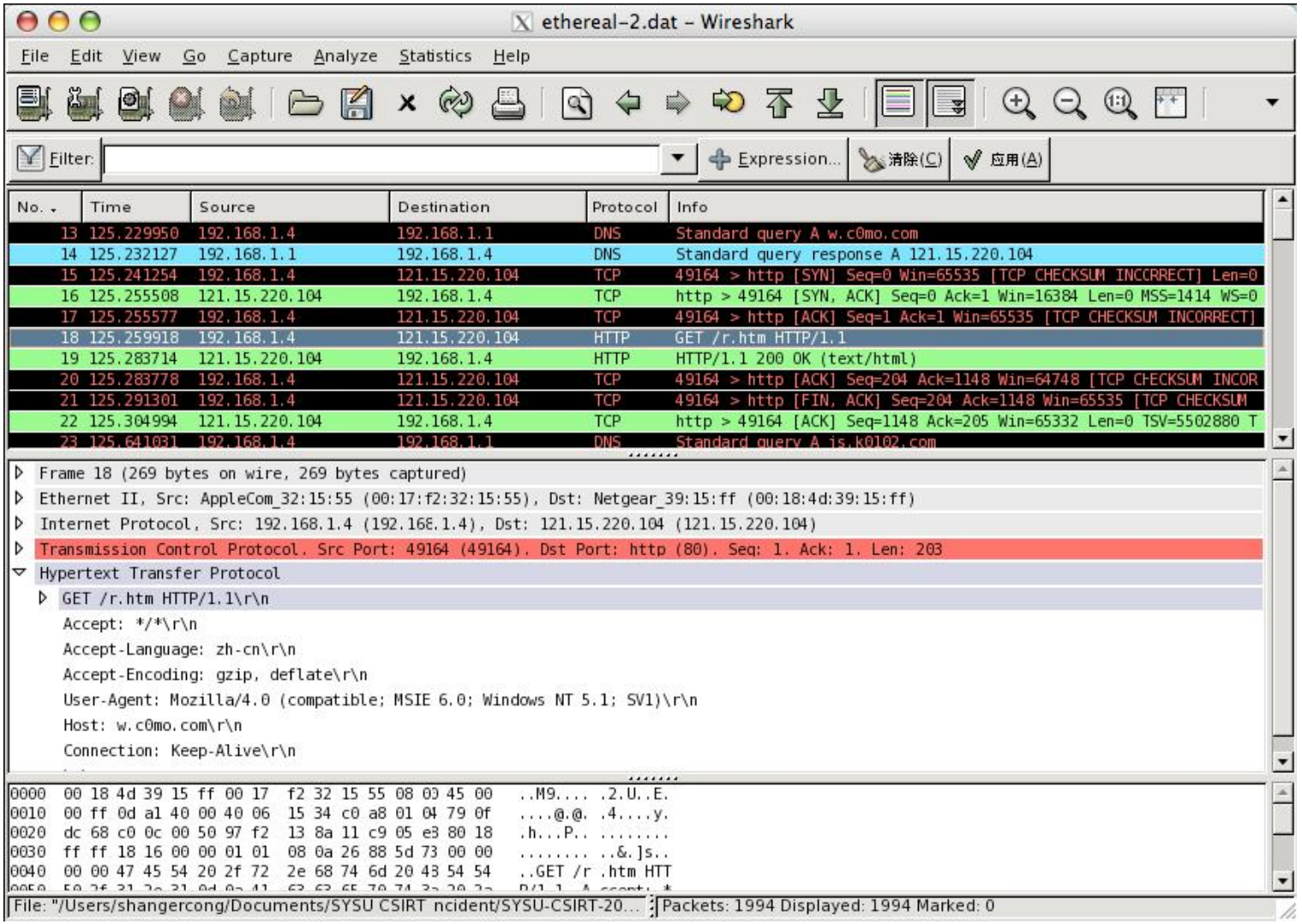
下载器木马使用域名下载木马(1)



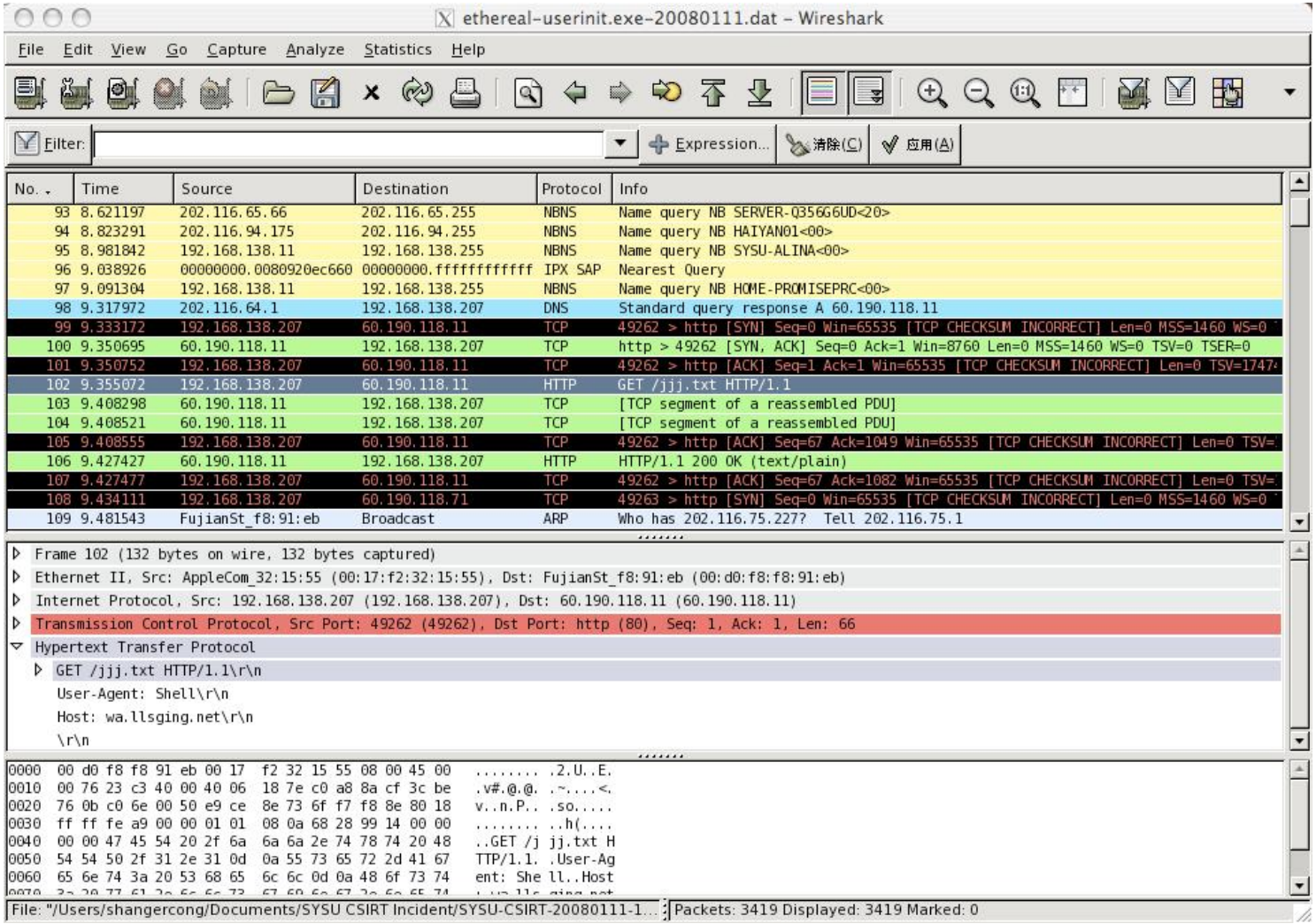
下载器木马使用域名下载木马(2)



下载器木马使用域名下载木马(3)



下载器木马使用域名下载木马(4)



下载器木马使用域名下载木马(5)

```
; <<>> DiG 9.3.4 <<>> w.c0mo.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33426
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;w.c0mo.com.                    IN      A

;; ANSWER SECTION:
w.c0mo.com.             2629    IN      A       121.15.220.104

;; Query time: 8 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Sat Dec 22 01:05:54 2007
;; MSG SIZE  rcvd: 44
```

```
; <<>> DiG 9.3.4 <<>> w.c0mo.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10411
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;w.c0mo.com.                    IN      A

;; ANSWER SECTION:
w.c0mo.com.             1144    IN      A       222.208.183.204

;; Query time: 7 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Thu Mar  6 18:57:40 2008
;; MSG SIZE  rcvd: 44
```

下载器木马使用域名下载木马(6)

```
; <<>> DiG 9.3.4 <<>> w.c0mo.com
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61769
;; flags: qr; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;w.c0mo.com.                    IN      A

;; ANSWER SECTION:
w.c0mo.com.             128     IN      A       59.37.71.85

;; Query time: 3 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Sun Mar 23 23:35:38 2008
;; MSG SIZE  rcvd: 44
```

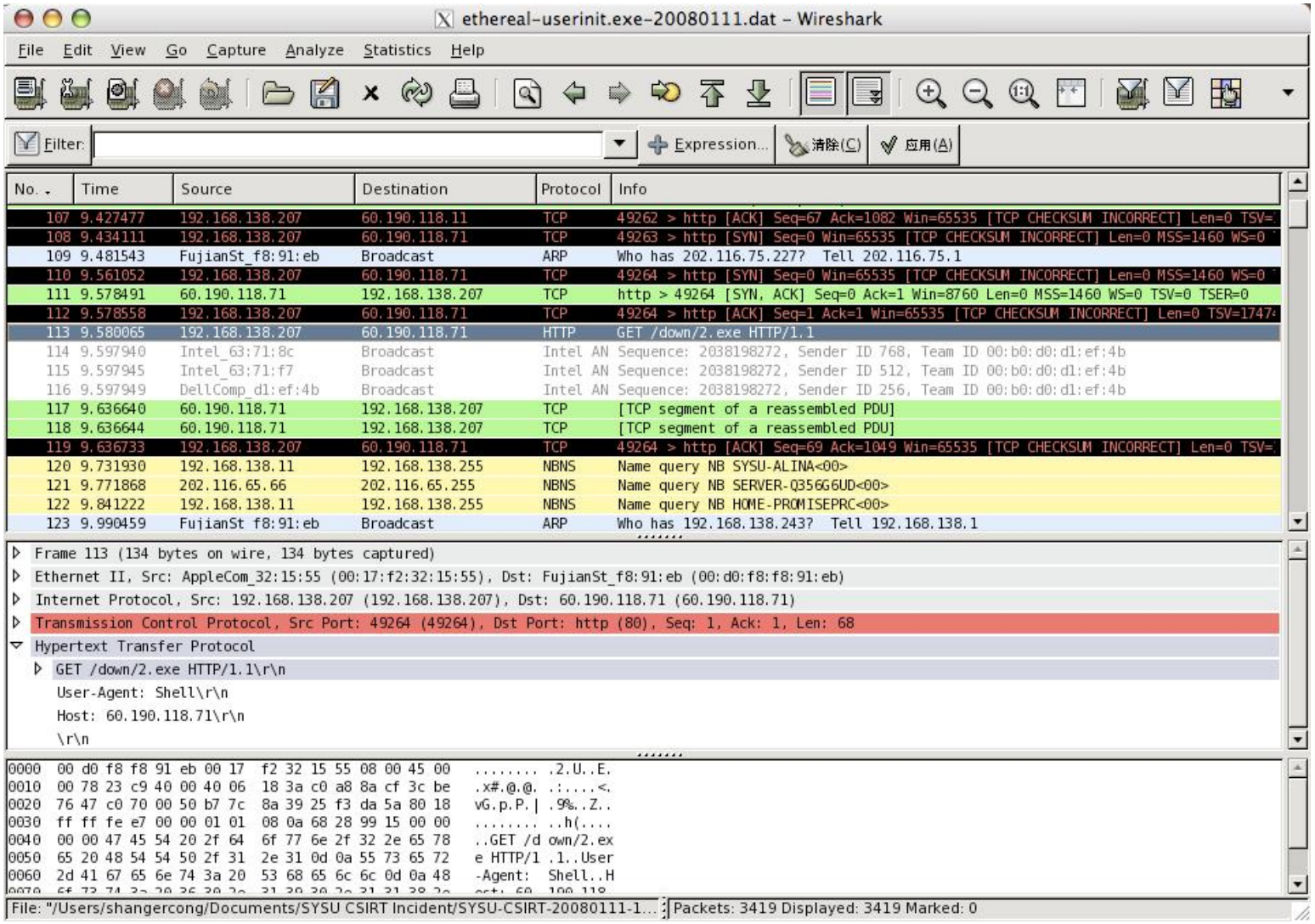
```
; <<>> DiG 9.3.4 <<>> @208.67.222.222 w.c0mo.com
; (1 server found)
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 7176
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;w.c0mo.com.                    IN      A

;; ANSWER SECTION:
w.c0mo.com.             1236    IN      A       125.65.165.133

;; Query time: 522 msec
;; SERVER: 208.67.222.222#53(208.67.222.222)
;; WHEN: Thu Mar 27 09:12:12 2008
;; MSG SIZE  rcvd: 44
```

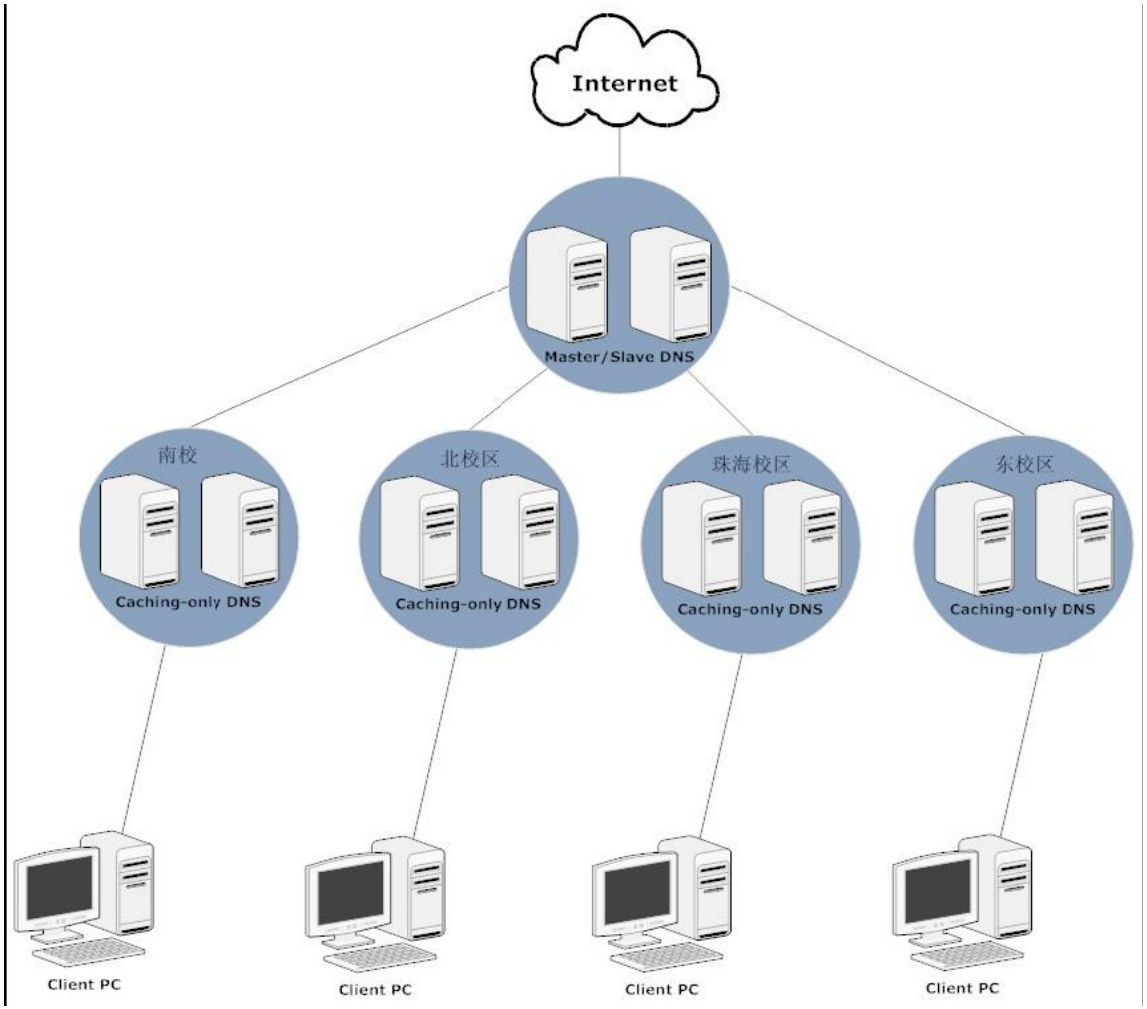
下载器木马不使用域名下载木马



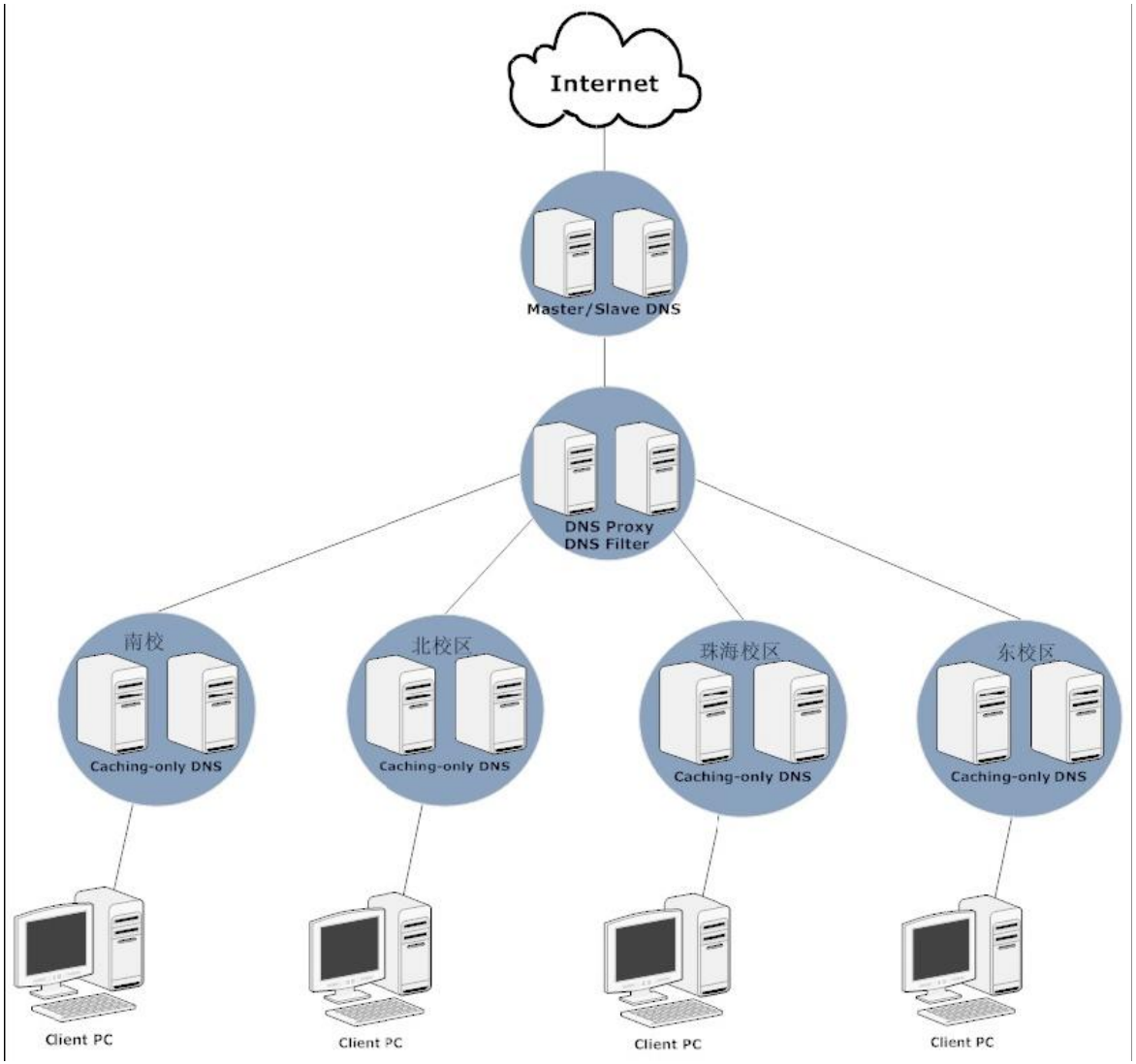
下载器木马使用域名带来的危害

- 信息犯罪者可以频繁更换域名对应的IP地址
- 绕过基于IP地址的ACL的封锁
- 需要使用DNS Blacklist封锁木马站点的域名
- dnrd (Domain Name Relay Daemon)，一般认为是一种DNS Proxy
- dnrd可以设置Blacklist，对Blacklist中的域名作出“权威的”应答，但并不会返回IP地址，达至封锁域名的目的

原DNS拓扑


Internet
Master/Slave DNS
南校
北校区
珠海校区
东校区
Caching-only DNS
Caching-only DNS
Caching-only DNS
Caching-only DNS
Client PC
Client PC
Client PC
Client PC

增加DNS Proxy过滤后的拓扑



Caching-only DNS配置

在BIND 9的配置文件中使用dnrd Blacklist:

```
    forwarders {
            202.116.64.119; // 转发到dnrd服务器
            202.116.64.120; // 转发到dnrd服务器
            202.116.64.2;
            202.116.64.1;
            202.116.64.3;
    };

    forward first;
```

DNS Proxy过滤

- 目前效果
  - drnd的Blacklist有40个域名
  - 每天约拒绝600-700次左右的查询
- 未来发展
  - DNS Blacklist需要维护
  - DNS需要有类似反垃圾邮件RBL信息共享机制
  - 与Stopbadware(www.stopbadware.org)联盟合作？

ARP欺骗木马的治理方法(1)

- 预防措施（主动）
  - 安全意识与安全文化
  - 系统及应用补丁
  - 定期“体检”
  - 宣传与教育
- 保护措施（半主动）
  - 防病毒及辅助清理软件
  - 防火墙及ARP防火墙
  - 交换机防ARP欺骗
  - 边界防火墙ACL过滤
  - DNS域名过滤
  - Web Content Filter
- 响应措施（被动）
  - ARPwatch
  - 三层交换机SNMPTrap/日志
  - 用户ARP防火墙日志与服务请求
  - CSIRT事件紧急响应
- 安全管理（战略）
  - 协调预防、保护与响应
  - 流程制订
  - 配置管理
  - 脆弱性及威胁跟踪与管理
  - 协作与信息共享

ARP欺骗木马的治理方法(2)

- 预防措施、保护措施、响应措施、安全管理之间具有相关性
- 响应措施（CSIRT事件紧急响应）可为保护措施提供依据（例如可提请修订病毒定义、封锁木马站点、发现更多的受害机器等）
- 响应措施（CSIRT事件紧急响应）也可为安全管理提供依据（脆弱性及威胁跟踪与管理协作与信息共享等）
- 安全管理可以协调预防、保护与响应
- ARP欺骗木马会随时间的推移而逐渐消亡，但新的威胁会随之而来，应以ARP欺骗木马及CSIRT紧急响做为突破口，完善高校的ISMS（信息安全管理体系）

信息安全需求的缺口大

- 东(大学城)校区学生助理考核65人参加
- 信息安全与防病毒部分平均分仅有79.13
- 超过90分的仅有4人
- 其他考核项目平均分均超过90分
- 关于违反《中华人民共和国治安管理处罚法》中有关计算机安全处罚的问题，答对率只有52%(34人答对)，答对率倒数第三

协作与信息共享

- forum.ccert.edu.cn是个很好的信息共享平台，是否可以就以下方面加强个院校的合作：
  - 威胁管理
    - 病毒样本分析
    - 恶意站点ACL管理
    - 恶意站点域名管理
  - 披露与公告