



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

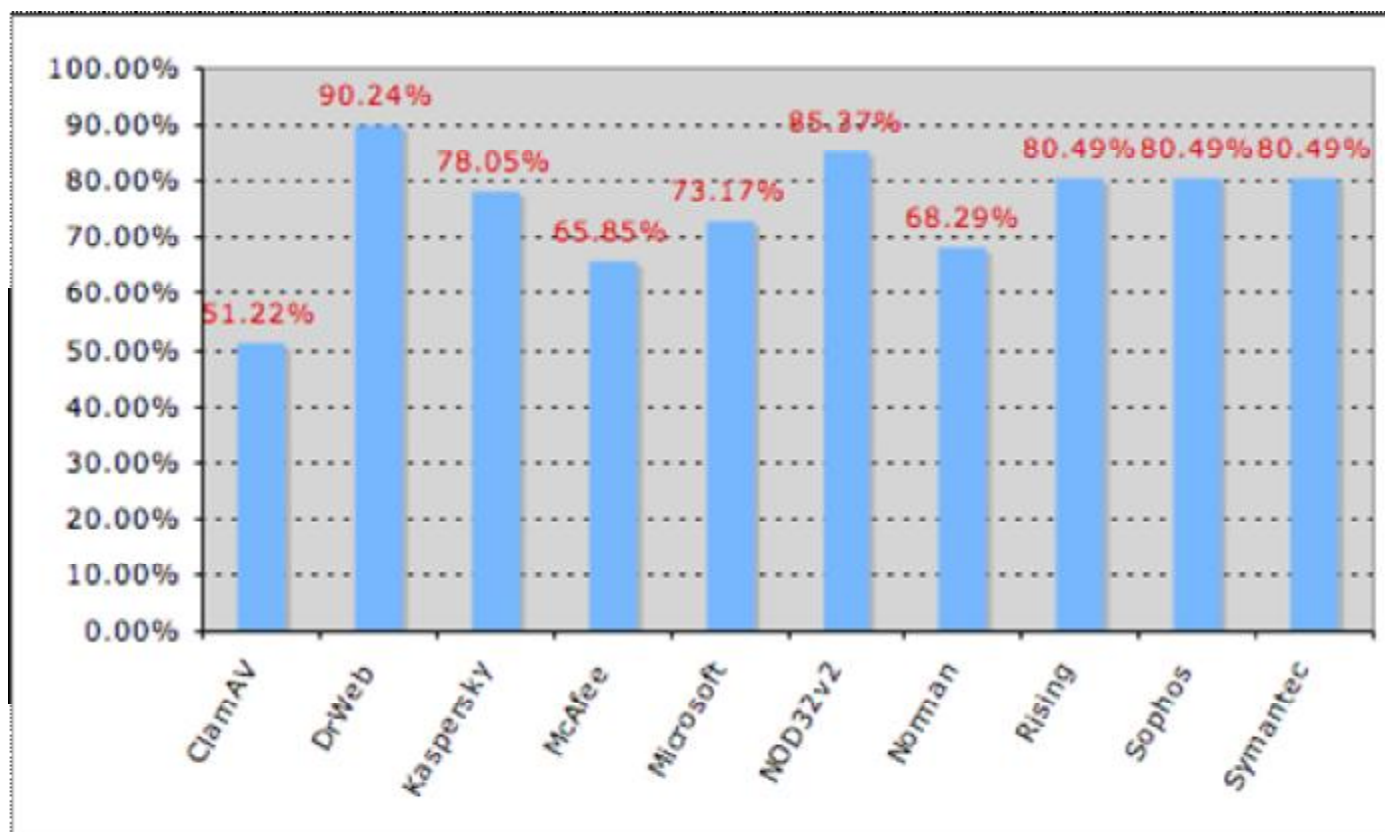


- 防病毒软件还是防病毒服务?
- ARP欺骗木马治理与对策



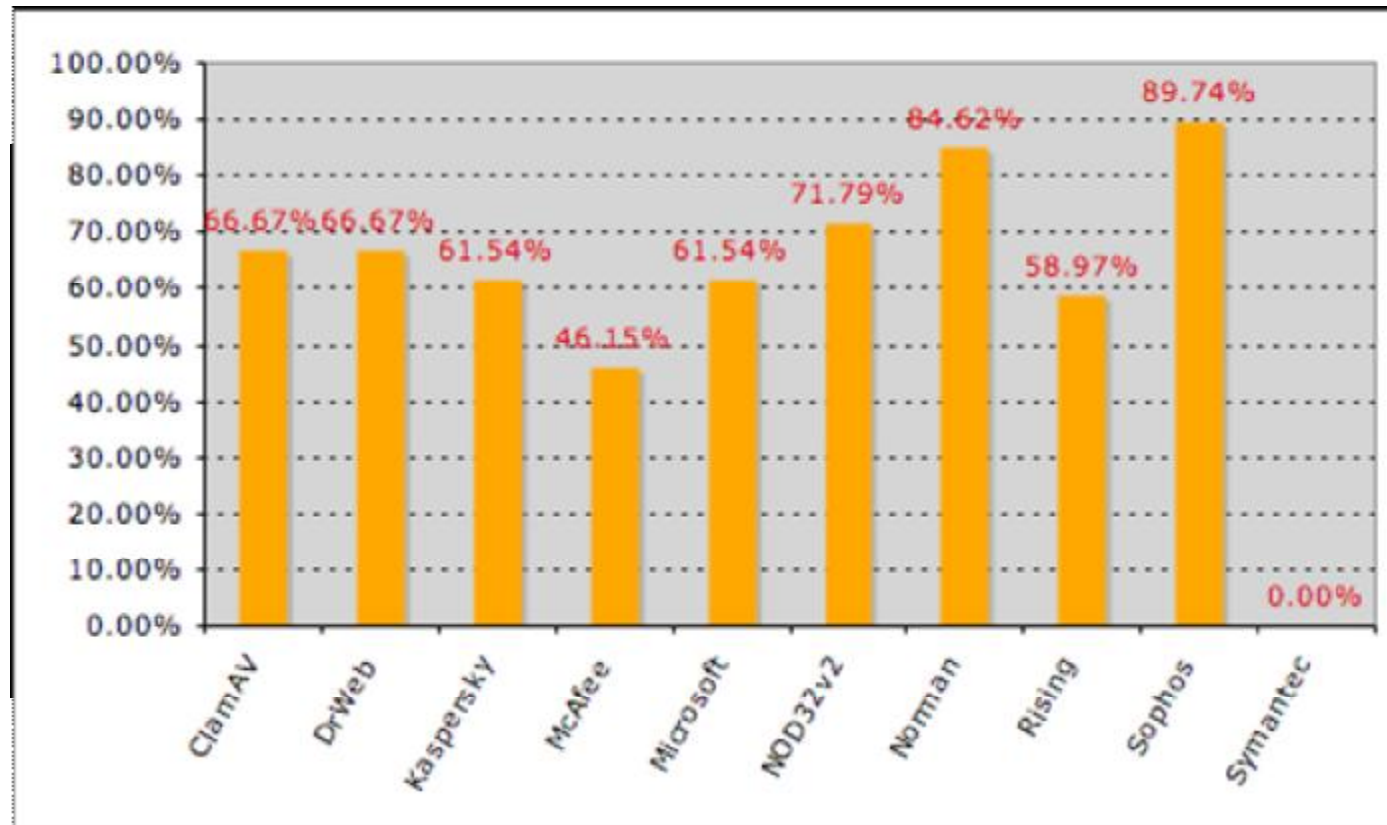
防病毒软件还是防病毒服务?

07'9-10提交VirusTotal 41个样本首次提交检出率



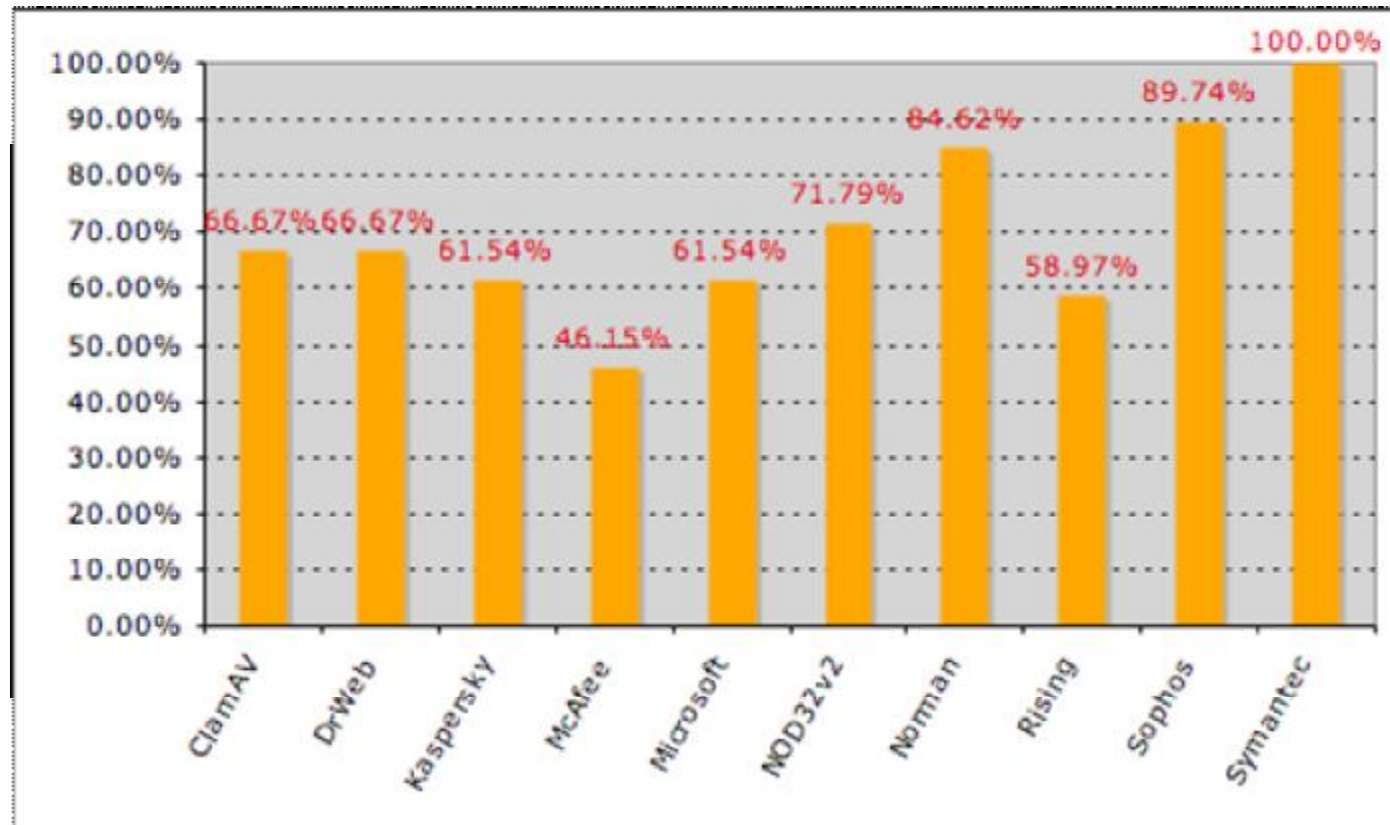
2007年9月-10月收集的41个病毒样本首次提交检出率统计

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



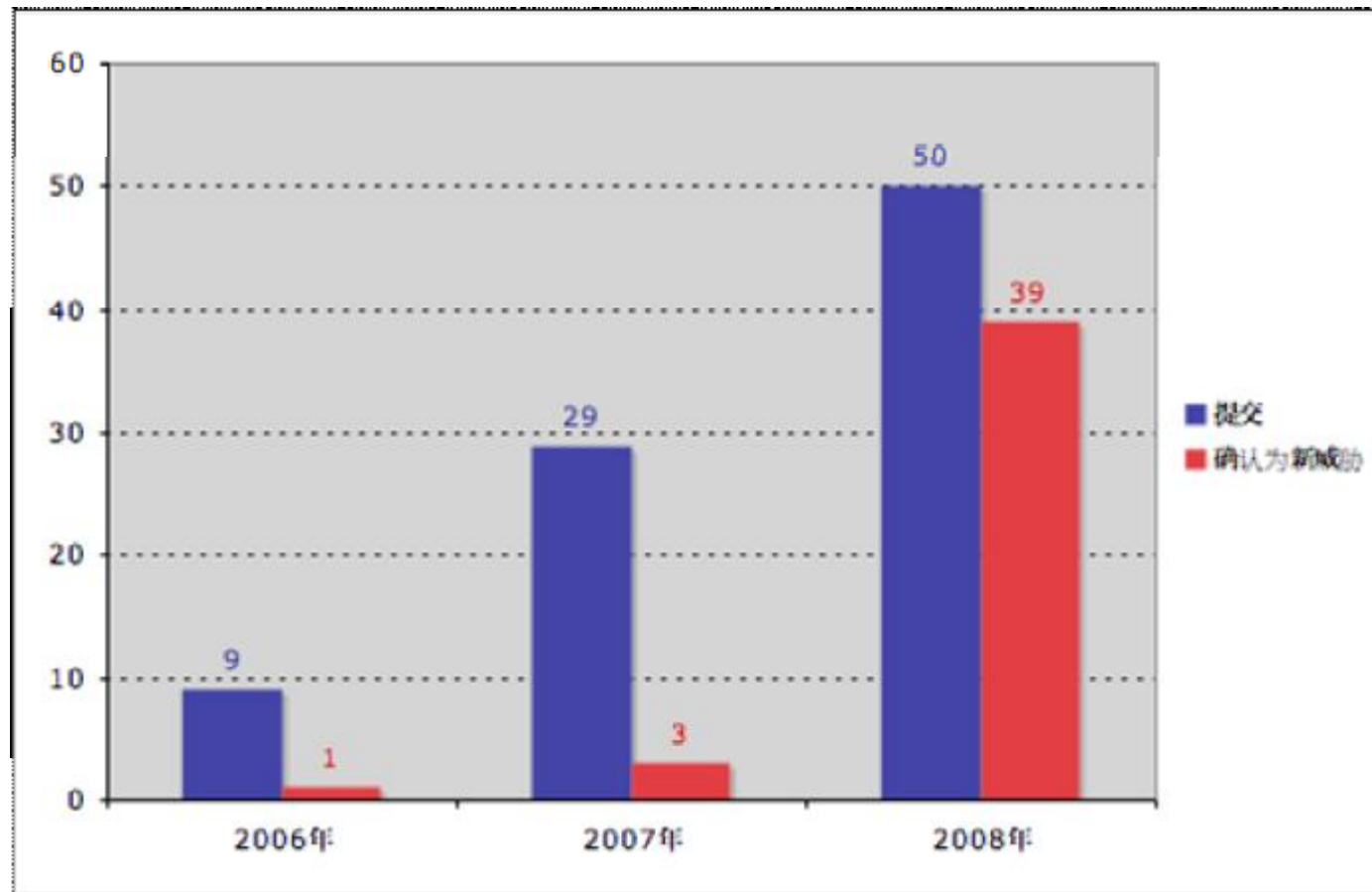
2008年1月-3月收集的39个样本Symantec首次无法检出

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

Organisations, whether private or public, are increasingly looking and making more information available electronically. There is a broad increase in reliance on IT systems.

This is coupled with an extraordinary increase in the use of online services. This is becoming an increasingly important part of many business. Lack of an internet presence can be detrimental to promotional success.

The increasing use of IT systems to store and process information makes keeping this information secure more important. One of the key shortcomings of organisations today is to ensure that staff act in an appropriate manner. This includes staff acting to keep sensitive information secure.

The Information Security Forum (ISF) is one of the leading independent authorities on information security. Through various key research, the ISF have defined several key ongoing processes of working that is essential to organisations, and defined means to ensure that the organisation that is taking behavioural change.

Copyrighted and the measurement of success

Approaches to raise awareness

The foundation to any framework for information security awareness is a sound security policy. Without an effective security policy, the use of systems and information, the resulting good behaviour is very hard.

Good practice standards place a strong emphasis on staff. An organisation with security measures in place should suggest that organisations implement the security policy. There is a growing emphasis on staff to ensure that they are fully aware of the importance of security. The importance of staff is highlighted in the ISF research, and the ISF has identified a number of key findings that are relevant to the ISF. These findings are:

- Understand, truly understand, who is responsible for the security policy.
- Understand, truly understand, who is responsible for the security policy.
- Understand, truly understand, who is responsible for the security policy.

Approaches to raise awareness

Retailer - fitting in with the culture

A large retailer explained why being flexible in the approach to information security awareness is important. They have large volumes of information about customers, such as their financial and credit card details. However, the retail sector does not have as strong a compliance culture as many other industry sectors, although Data Protection and PCI compliance are key.

The flexible nature of the work from retailers delivering an effective awareness programme is challenging. The level of computer literacy varies widely and the age of staff ranges from school leavers to retirement age. Messages need to be tailored accordingly. Staff broadly comprise of three different groups. Firstly, in shops and outlets, staff deal with customers and use till and stock systems, and have generally less IT experience. Secondly, head office staff deal with IT systems and are generally users of computer equipment. Finally, the technical teams within IT that have powerful access rights.

A risk-based approach is used to define messages. The key risks that are present for each group of users are analysed. Based on this, key messages for each year are selected and communication plans put in place. Each group faces different risks, so the messages for each group are different.

A wide range of techniques are used due to the diversity of the staff. Information security is built into staff induction training. Key messages that people are informed of their responsibilities as they join. In store outlets posters for

Information security awareness initiatives: Current practice and the measurement of success

July 2007

enisa
European Network and Information Security Agency

What techniques have proved effective at raising information security awareness?

Technique	Score
Classroom training	5.1
Individual personal development plan	4.8
Security policy/standards	4.7
Poster campaigns	4.6
Regular email or newsletter	4.5
Computer-based training	4.4
Leaflets	4.3
Internet sites	4.2
Guides	4.1
Procedural manuals (e.g. sign)	4.0

Part of running an effective programme is to get the right messages to the right people. This understanding of each group's current information issues and the extent to which they are aware is key. Surprisingly, only 36% of respondents have

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)



COMPUTER AND NETWORK
SECURITY
TASK FORCE



STAYSAFEONLINE.org
National Cyber Security Alliance



2006 - 2007 Computer Security Awareness Video Contest

Computer Security Awareness
Video Contest 2007





安全意识与教育(3)





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

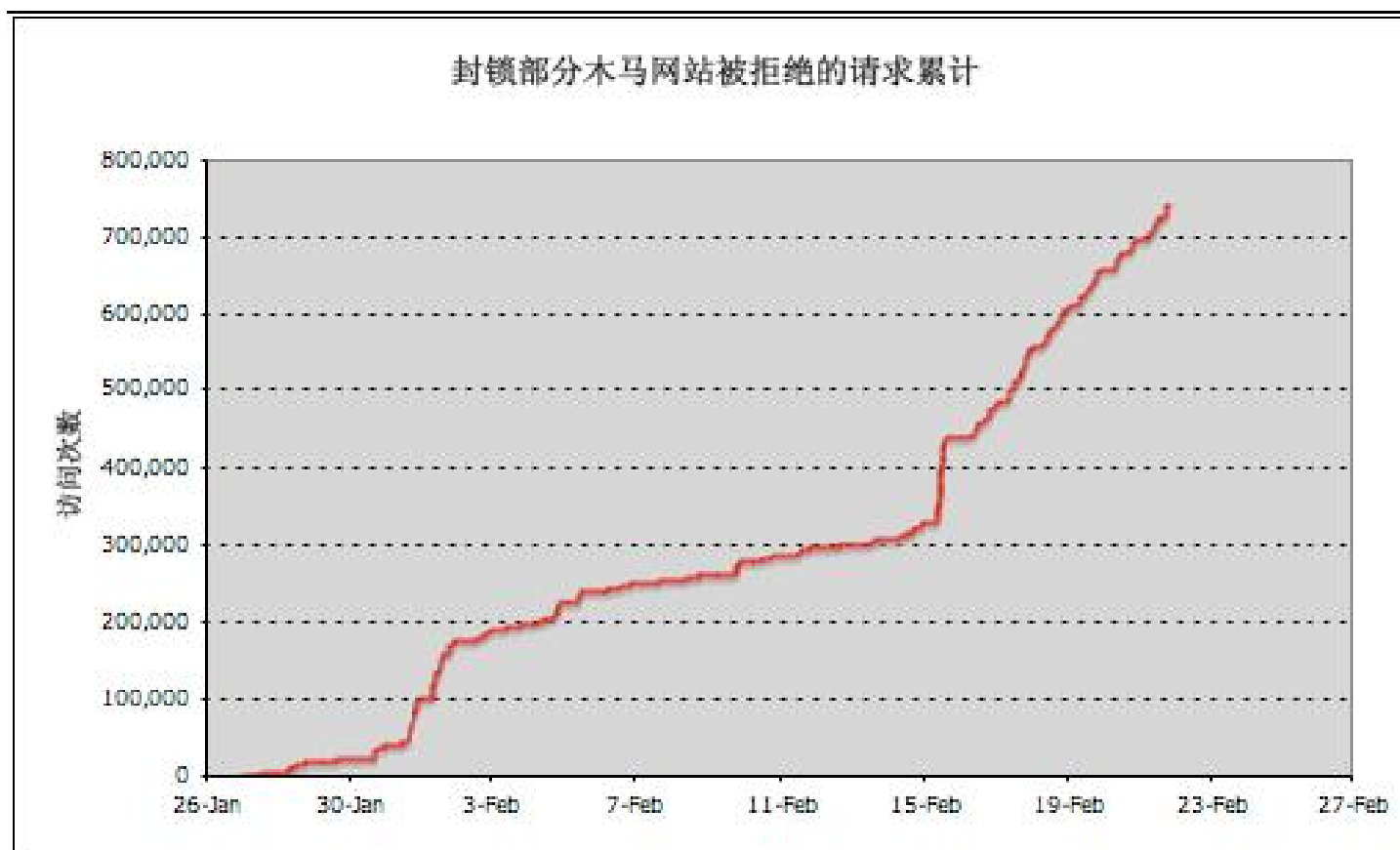


ARP欺骗的目的和类型

- 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。

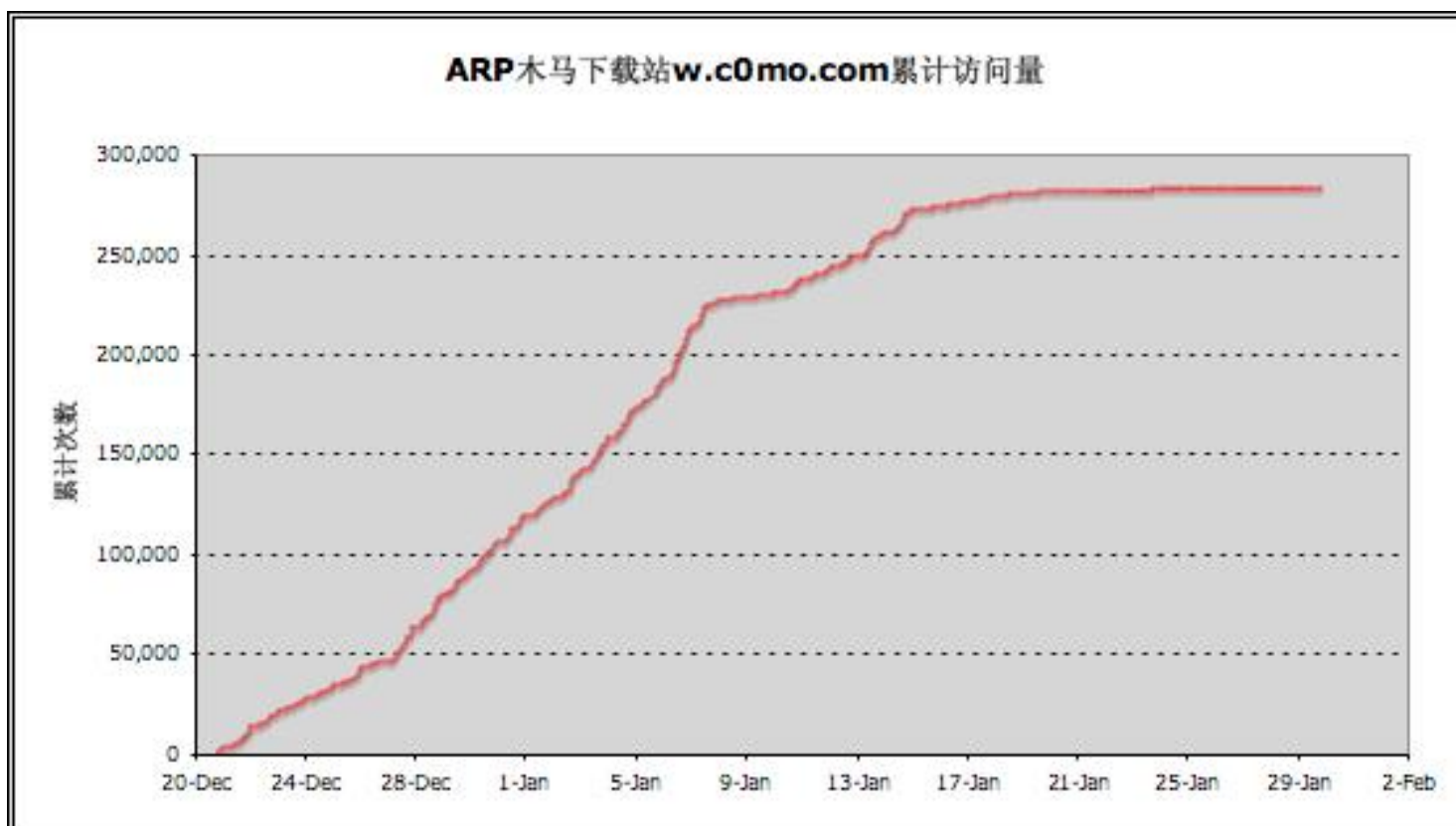


封锁木马网站的有效性



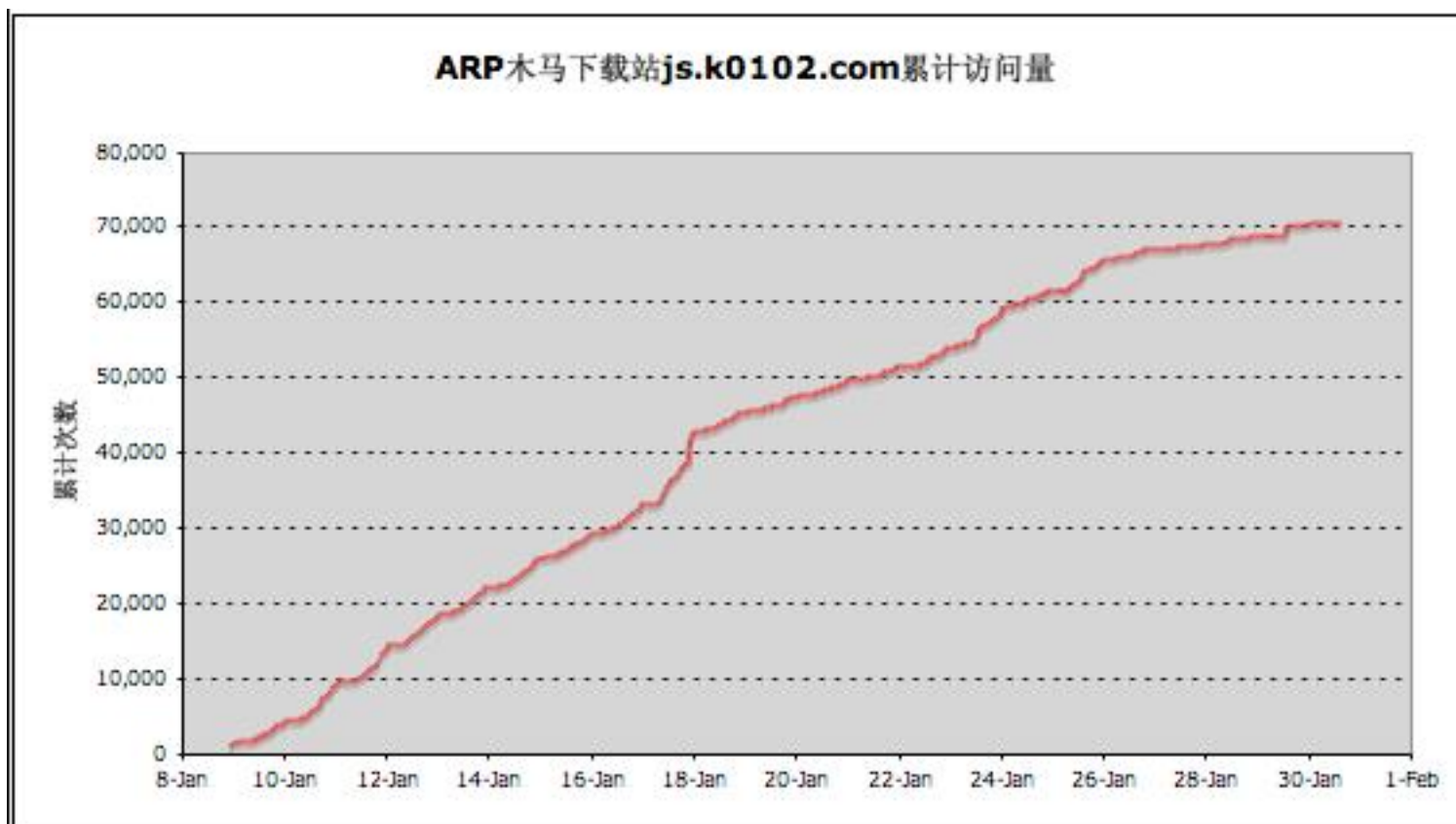


下载器木马使用域名下载木马(1)





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)

The image shows a Wireshark capture of network traffic. The main pane displays a list of packets with the following details:

No.	Time	Source	Destination	Protocol	Info
13	125.229950	192.168.1.4	192.168.1.1	DNS	Standard query A w.c0mo.com
14	125.232127	192.168.1.1	192.168.1.4	DNS	Standard query response A 121.15.220.104
15	125.241254	192.168.1.4	121.15.220.104	TCP	49164 > http [SYN, ACK] Seq=0 Win=65535 [TCP CHECKSUM INCCRRECT] Len=0
16	125.255508	121.15.220.104	192.168.1.4	TCP	http > 49164 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1414 WS=0
17	125.255577	192.168.1.4	121.15.220.104	TCP	49164 > http [ACK] Seq=1 Ack=1 Win=65535 [TCP CHECKSUM INCORRECT]
18	125.259918	192.168.1.4	121.15.220.104	HTTP	GET /r.htm HTTP/1.1
19	125.283714	121.15.220.104	192.168.1.4	HTTP	HTTP/1.1 200 OK (text/html)
20	125.283778	192.168.1.4	121.15.220.104	TCP	49164 > http [ACK] Seq=204 Ack=1148 Win=64748 [TCP CHECKSUM INCOR]
21	125.291301	192.168.1.4	121.15.220.104	TCP	49164 > http [FIN, ACK] Seq=204 Ack=1148 Win=65535 [TCP CHECKSUM
22	125.304994	121.15.220.104	192.168.1.4	TCP	http > 49164 [ACK] Seq=1148 Ack=205 Win=65332 Len=0 TSV=5502880 T
23	125.641031	192.168.1.4	192.168.1.1	DNS	Standard query A is.k0102.com

The packet details pane for frame 18 shows the following information:

- Frame 18 (269 bytes on wire, 269 bytes captured)
- Ethernet II, Src: AppleCom_32:15:55 (00:17:f2:32:15:55), Dst: Netgear_39:15:ff (00:18:4d:39:15:ff)
- Internet Protocol, Src: 192.168.1.4 (192.168.1.4), Dst: 121.15.220.104 (121.15.220.104)
- Transmission Control Protocol, Src Port: 49164 (49164), Dst Port: http (80), Seq: 1, Ack: 1, Len: 203
- Hypertext Transfer Protocol
 - GET /r.htm HTTP/1.1\r\n
 - Accept: */*\r\n
 - Accept-Language: zh-cn\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)\r\n
 - Host: w.c0mo.com\r\n
 - Connection: Keep-Alive\r\n

The packet bytes pane shows the raw data of the GET request:

```
0000 00 18 4d 39 15 ff 00 17 f2 32 15 55 08 03 45 00 ..M9.... .2.U..E.  
0010 00 ff 0d a1 40 00 40 06 15 34 c0 a8 01 04 79 0f ....@.@. .4....y.  
0020 dc 68 c0 0c 00 50 97 f2 13 8a 11 c9 05 e3 80 18 .h...P... ..  
0030 ff ff 18 16 00 00 01 01 08 0a 26 88 5d 73 00 00 ..... ..&.js..  
0040 00 00 47 45 54 20 2f 72 2e 68 74 6d 20 43 54 54 ..GET /r.htm HTT  
0050 50 2e 21 2e 21 04 0e 41 62 62 65 70 74 2e 20 2e 0/1.1 A cept: *
```




下载器木马使用域名下载木马(4)

ethereal-userinit.exe-20080111.dat - Wireshark

File Edit View Go Capture Analyze Statistics Help

Filter: + Expression... 清除(C) 应用(A)

No. .	Time	Source	Destination	Protocol	Info
93	8.621197	202.116.65.66	202.116.65.255	NBNS	Name query NB SERVER-Q35666UD<20>
94	8.823291	202.116.94.175	202.116.94.255	NBNS	Name query NB HAIYAN01<00>
95	8.981842	192.168.138.11	192.168.138.255	NBNS	Name query NB SYSU-ALINA<00>
96	9.038926	00000000.0080920ec660	00000000.ffffffffffff	IPX SAP	Nearest Query
97	9.091304	192.168.138.11	192.168.138.255	NBNS	Name query NB HOME-PROMISEPRC<00>
98	9.317972	202.116.64.1	192.168.138.207	DNS	Standard query response A 60.190.118.11
99	9.333172	192.168.138.207	60.190.118.11	TCP	49262 > http [SYN] Seq=0 Win=65535 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460 WS=0
100	9.350695	60.190.118.11	192.168.138.207	TCP	http > 49262 [SYN, ACK] Seq=0 Ack=1 Win=8760 Len=0 MSS=1460 WS=0 TSV=0
101	9.350752	192.168.138.207	60.190.118.11	TCP	49262 > http [ACK] Seq=1 Ack=1 Win=65535 [TCP CHECKSUM INCORRECT] Len=0 TSV=1747
102	9.355072	192.168.138.207	60.190.118.11	HTTP	GET /jjj.txt HTTP/1.1
103	9.408298	60.190.118.11	192.168.138.207	TCP	[TCP segment of a reassembled PDU]
104	9.408521	60.190.118.11	192.168.138.207	TCP	[TCP segment of a reassembled PDU]
105	9.408555	192.168.138.207	60.190.118.11	TCP	49262 > http [ACK] Seq=67 Ack=1049 Win=65535 [TCP CHECKSUM INCORRECT] Len=0 TSV=
106	9.427427	60.190.118.11	192.168.138.207	HTTP	HTTP/1.1 200 OK (text/plain)
107	9.427477	192.168.138.207	60.190.118.11	TCP	49262 > http [ACK] Seq=67 Ack=1082 Win=65535 [TCP CHECKSUM INCORRECT] Len=0 TSV=
108	9.434111	192.168.138.207	60.190.118.11	TCP	49263 > http [SYN] Seq=0 Win=65535 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460 WS=0
109	9.481543	FujianSt_f8:91:eb	Broadcast	ARP	Who has 202.116.75.227? Tell 202.116.75.1

Frame 102 (132 bytes on wire, 132 bytes captured)

- Ethernet II, Src: AppleCom_32:15:55 (00:17:f2:32:15:55), Dst: FujianSt_f8:91:eb (00:d0:f8:f8:91:eb)
- Internet Protocol, Src: 192.168.138.207 (192.168.138.207), Dst: 60.190.118.11 (60.190.118.11)
- Transmission Control Protocol, Src Port: 49262 (49262), Dst Port: http (80), Seq: 1, Ack: 1, Len: 66
- Hypertext Transfer Protocol
 - GET /jjj.txt HTTP/1.1\r\n
 - User-Agent: Shell\r\n
 - Host: wa.llsging.net\r\n
 - \r\n

0000 00 d0 f8 f8 91 eb 00 17 f2 32 15 55 08 00 45 002.U...E.
0010 00 76 23 c3 40 00 40 06 18 7e c0 a8 8a cf 3c be .v#.@. .>...<
0020 76 0b c0 6e 00 50 e9 ce 8e 73 6f f7 f8 8e 80 18 v..n.P..so....
0030 ff ff fe a9 00 00 01 01 08 0a 68 28 99 14 00 00h(...
0040 00 00 47 45 54 20 2f 6a 6a 6a 2e 74 78 74 20 48 ..GET /j jj.txt H
0050 54 54 50 2f 31 2e 31 0d 0a 55 73 65 72 2d 41 67 TTP/1.1. .User-Ag
0060 65 6e 74 3a 20 53 68 65 6c 6c 0d 0a 48 6f 73 74 ent: She ll..Host
0070 2a 20 77 61 20 6a 6a 73 67 6a 6a 67 2a 6a 6a 74 ..llsging.net

File: "/Users/shangercong/Documents/SYSU CSIRT Incident/SYSU-CSIRT-20080111-1..."; Packets: 3419 Displayed: 3419 Marked: 0



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

The image shows a Wireshark capture of network traffic. The main pane displays a list of packets. Packet 113 is highlighted, showing a GET request for a file named '2.exe' over HTTP. The details pane below shows the structure of the packet, including Ethernet II, Internet Protocol, and Hypertext Transfer Protocol layers. The raw data pane at the bottom shows the hexadecimal and ASCII representation of the packet data.

No.	Time	Source	Destination	Protocol	Info
107	9.427477	192.168.138.207	60.190.118.11	TCP	49262 > http [ACK] Seq=67 Ack=1082 Win=65535 [TCP CHECKSUM INCORRECT] Len=0 TSV=
108	9.434111	192.168.138.207	60.190.118.71	TCP	49263 > http [SYN] Seq=0 Win=65535 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460 WS=0
109	9.481543	FujianSt_f8:91:eb	Broadcast	ARP	Who has 202.116.75.227? Tell 202.116.75.1
110	9.561052	192.168.138.207	60.190.118.71	TCP	49264 > http [SYN] Seq=0 Win=65535 [TCP CHECKSUM INCORRECT] Len=0 MSS=1460 WS=0
111	9.578491	60.190.118.71	192.168.138.207	TCP	http > 49264 [SYN, ACK] Seq=0 Ack=1 Win=8760 Len=0 MSS=1460 WS=0 TSV=0 TSER=0
112	9.578558	192.168.138.207	60.190.118.71	TCP	49264 > http [ACK] Seq=1 Ack=1 Win=65535 [TCP CHECKSUM INCORRECT] Len=0 TSV=1747
113	9.580065	192.168.138.207	60.190.118.71	HTTP	GET /down/2.exe HTTP/1.1
114	9.597940	Intel_63:71:8c	Broadcast	Intel AN	Sequence: 2038198272, Sender ID 768, Team ID 00:b0:d0:d1:ef:4b
115	9.597945	Intel_63:71:f7	Broadcast	Intel AN	Sequence: 2038198272, Sender ID 512, Team ID 00:b0:d0:d1:ef:4b
116	9.597949	DellComp_d1:ef:4b	Broadcast	Intel AN	Sequence: 2038198272, Sender ID 256, Team ID 00:b0:d0:d1:ef:4b
117	9.636640	60.190.118.71	192.168.138.207	TCP	[TCP segment of a reassembled PDU]
118	9.636644	60.190.118.71	192.168.138.207	TCP	[TCP segment of a reassembled PDU]
119	9.636733	192.168.138.207	60.190.118.71	TCP	49264 > http [ACK] Seq=69 Ack=1049 Win=65535 [TCP CHECKSUM INCORRECT] Len=0 TSV=
120	9.731930	192.168.138.11	192.168.138.255	NBNS	Name query NB SYSU-ALINA<00>
121	9.771868	202.116.65.66	202.116.65.255	NBNS	Name query NB SERVER-Q356G6UD<00>
122	9.841222	192.168.138.11	192.168.138.255	NBNS	Name query NB HOME-PROMISEPRC<00>
123	9.990459	FujianSt_f8:91:eb	Broadcast	ARP	Who has 192.168.138.243? Tell 192.168.138.1

Frame 113 (134 bytes on wire, 134 bytes captured)

- Ethernet II, Src: AppleCom_32:15:55 (00:17:f2:32:15:55), Dst: FujianSt_f8:91:eb (00:d0:f8:f8:91:eb)
- Internet Protocol, Src: 192.168.138.207 (192.168.138.207), Dst: 60.190.118.71 (60.190.118.71)
- Transmission Control Protocol, Src Port: 49264 (49264), Dst Port: http (80), Seq: 1, Ack: 1, Len: 68
- Hypertext Transfer Protocol
 - GET /down/2.exe HTTP/1.1\r\n
 - User-Agent: Shell\r\n
 - Host: 60.190.118.71\r\n
 - \r\n

```
0000  00 d0 f8 f8 91 eb 00 17 f2 32 15 55 08 00 45 00  .... .2.U..E.
0010  00 78 23 c9 40 00 40 06 18 3a c0 a8 8a cf 3c be  .x#.@. ....<
0020  76 47 c0 70 00 50 b7 7c 8a 39 25 f3 da 5a 80 18  vG.p.P. | .9%.Z..
0030  ff ff fe e7 00 00 01 01 08 0a 68 28 99 15 00 00  .... ..h(....
0040  00 00 47 45 54 20 2f 64 6f 77 6e 2f 32 2e 65 78  ..GET /d own/2.ex
0050  65 20 48 54 54 50 2f 31 2e 31 0d 0a 55 73 65 72  e HTTP/1 .l..User
0060  2d 41 67 65 6e 74 3a 20 53 68 65 6c 6c 0d 0a 48  -Agent: Shell..H
0070  6f 72 74 20 20 2f 20 20 21 20 20 20 21 21 20 20  ...f. 60 100 110
```

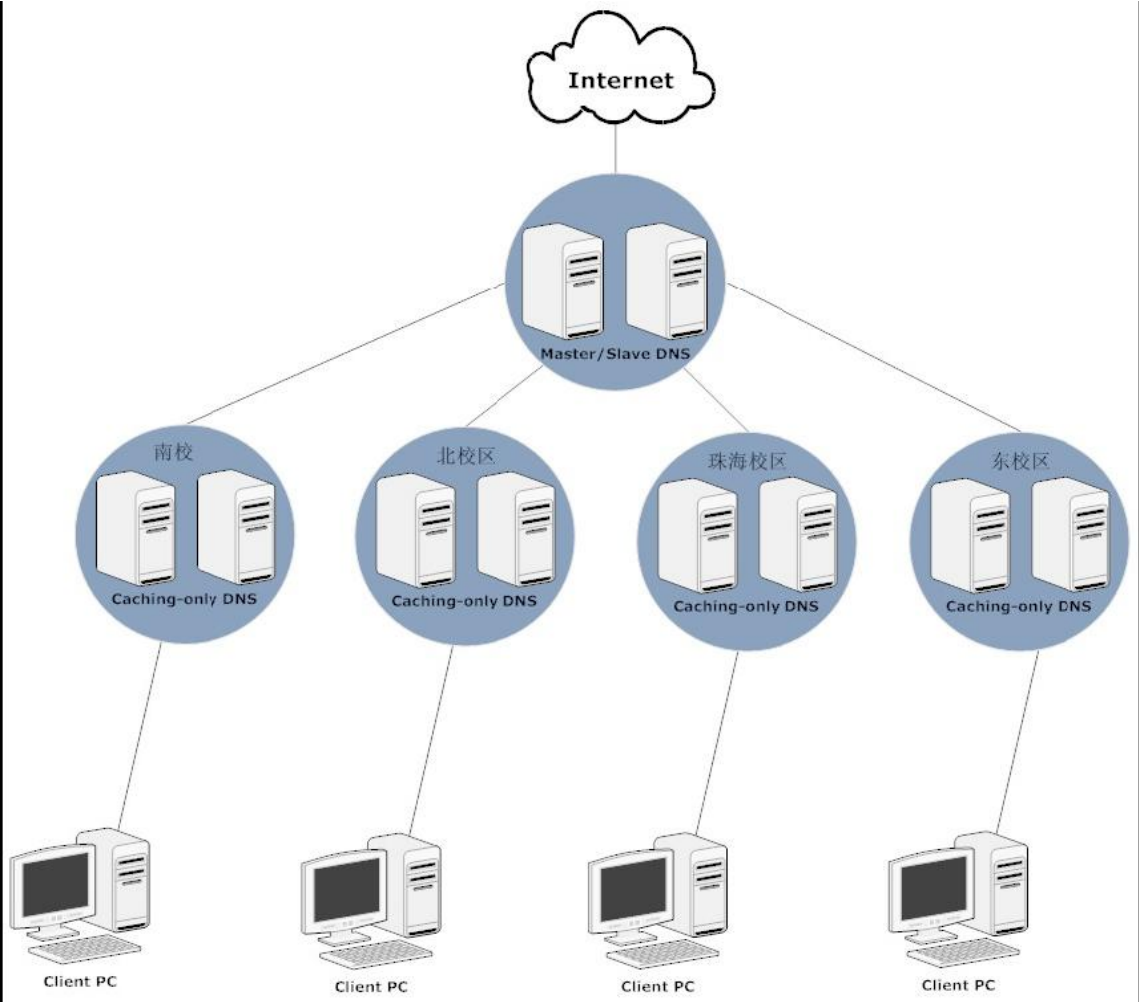
File: /Users/shangercong/Documents/SYSU CSIRT Incident/SYSU-CSIRT-20080111-1...; Packets: 3419 Displayed: 3419 Marked: 0



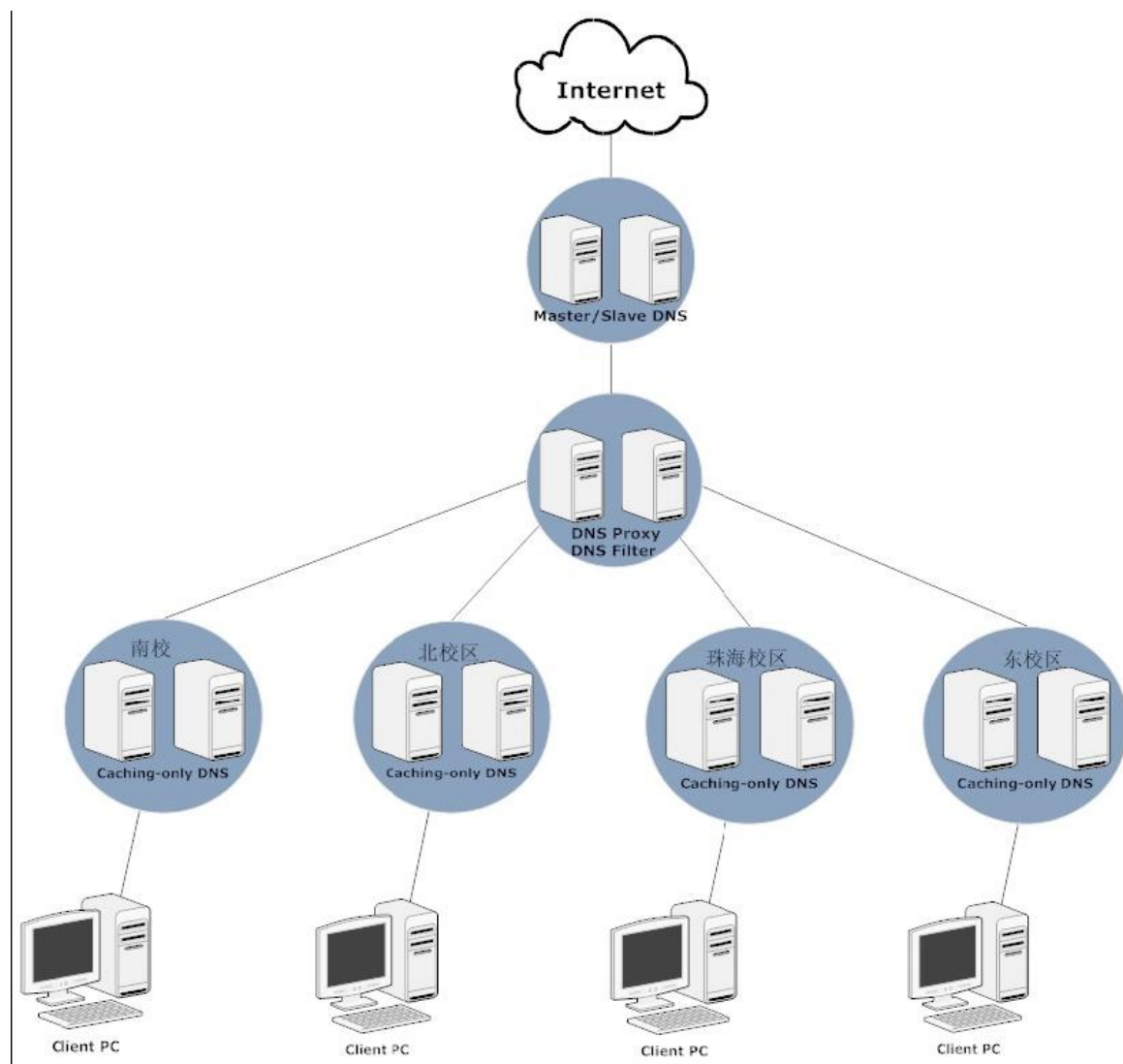
下载器木马使用域名带来的危害

- ❑ 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



增加DNS Proxy过滤后的拓扑





Caching-only DNS配置

在BIND 9的配置文件中使用时使用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**（信息安全管理体糸）



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