

病毒，间谍软件，广告软件和 Rootkit

褚诚云
软件开发组长
微软Windows 安全部门
chchu@microsoft.com

提纲

- 安全现状
- 有害软件（病毒）
- 间谍软件，广告软件
- Rootkit
- Phishing
- 监测和防护
- Q&A

安全现状

- 有害软件（病毒）增长的速度加快
- 间谍软件，广告软件泛滥成灾
- Rootkit技术发展迅速
- 针对普通用户的Phishing攻击

用户和企业

- 没有做好相应准备
 - 系统没有安装最新的安全补丁
 - 用户认为间谍软件，广告软件是免费软件的一部分

有害软件（病毒）的最新统计数据

- 数据来源 Symantec 2005年3月发布的互联网安全报告
<http://enterprisesecurity.symantec.com/content.cfm?articleid=1539>
- Q304/Q105有1403新的安全漏洞被发现
 - 较前六个月相比，增幅13%
 - 97%安全漏洞的严重级别是中或高
- 04下半年发现7630新的有害软件
 - 较前六个月相比，增幅64%
- 在04下半年发现有害软件中，试图窃取用户机密信息
 - 较前六个月相比，从44%增长到54%
- 单个组织每日平均被攻击次数
 - 较前六个月相比，从10.6增长到13.6

目的和攻击模式

- 目的：
 - 以前：登上报纸的头版头条
 - 现在：具体化的实际利益
- 攻击模式：
 - 以前：感染范围大，速度快
 - 现在：受控传播，针对特定用户
- Israel的安全事件
<http://www.msnbc.msn.com/id/8145520/>
- Zotob

有害软件分类

- 后门 -- Backdoor
- 木马 -- Trojan
- 蠕虫 -- Worm
- 文件感染剂 -- File infector (virus)

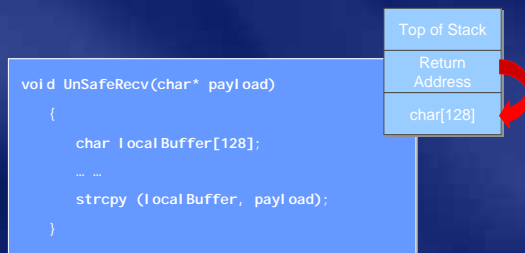
传播方式

- 利用操作系统的安全漏洞
- 社会工程? Social Engineering

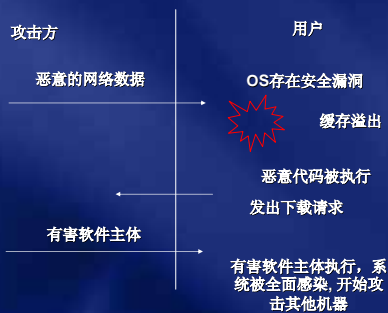
系统安全漏洞

- 缓存溢出 (Buffer Overrun)
 - Code Red: IIS缓存溢出
 - Blaster: DCOM RPC缓存溢出
 - Zotob: PnP缓存溢出

堆栈缓存溢出



典型攻击模式

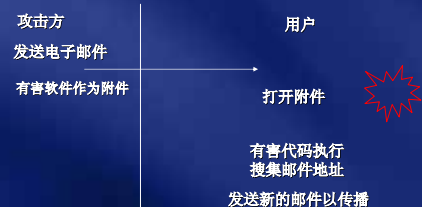


社会工程

- 攻击者通过某种手段, 例如虚假信息, 诱使用户执行一定的动作, 已达到控制系统, 窃取信息的目的
- 用户参与

典型攻击模式

邮件蠕虫

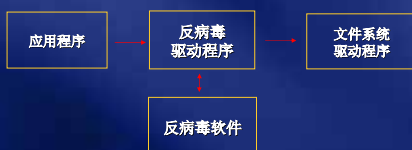


反病毒软件

- 文件扫描
- 基于特征代码 (signature)

实时防护

- 反病毒驱动程序截获应用程序的文件调用
- 监控I/O操作, 以便反病毒软件扫描文件



局限性

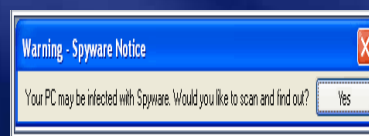
- 反病毒软件工作基于病毒样本的特征代码
 - 对于小规模传播的病毒, 可能没有特征代码
 - 病毒爆发和反病毒软件公司提供特征代码之间有时间间隔
- 仅依靠反病毒软件保护系统安全是不完善的

间谍软件/广告软件

- 间谍软件
 - 未经用户允许, 有以下行为的软件: 广告, 收集用户个人信息, 修改系统配置等等。
- 广告软件
 - 通过Banner和Popup显示广告的软件

传播途径

- 电子邮件邀请访问特定的网站, 或是运行附件
- 附加在其它软件中一起安装
- 通过弹出对话框或其它手段诱使用户安装



感染间谍软件的症状

- 广告框总是自动弹出
- IE的缺省主页和搜索配置未经允许被修改
- IE出现不熟悉的工具条，无法被正常删除
- 计算机性能下降
- 操作系统频繁崩溃

反间谍软件

- 和反病毒软件类似，主要是基于对文件的扫描。
- 扫描基于间谍软件特征代码的数据库
- <http://www.microsoft.com/athome/security/spyware/default.mspx>

防护措施

- 安装反间谍软件
- 尽量从正式网站下载软件
- 注意IE中Internet secure zone的配置
- 使用右上角的“X”关闭弹出框

Rootkit

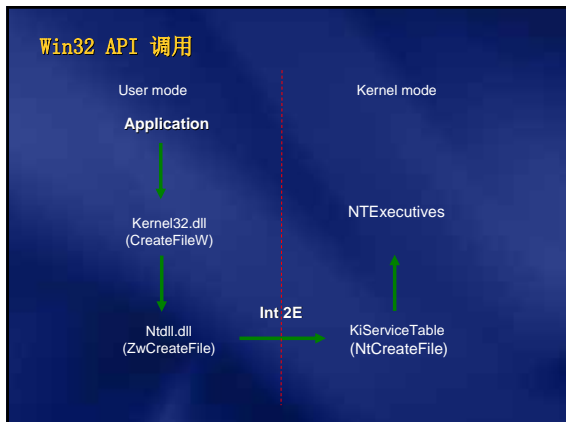
- 历史
 - 术语来自于Unix系统。最早的一个版本是出现在SunOS 4
- 用于修改操作系统，以改变操作系统的表现行为的工具软件。而这种改变，往往不是操作系统设计时所期望的

隐藏信息

- Rootkit可用于隐藏以下系统信息：
 - 运行进程
 - 服务
 - TCP/IP端口
 - 文件
 - 注册信息Registry
 - 用户帐号

新的威胁

- 越来越多的Windows系统的Rootkit
- 越来越多的有害软件，间谍软件和Rootkit绑定



- ### 类型
- User-Mode API 截获
 - Kernel-Mode API 截获
 - Kernel-Mode 数据结构修改

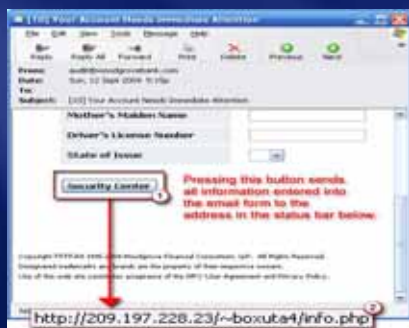
- ### 检测Rootkit
- Offline OS检测
 - API副作用检测
 - Rootkit检测工具
 - Strider/Ghostbuster, MS Research
 - RootkitRevealer, Sysinternals

- ### 删除Rootkit
- 官方提供的工具
 - 重新安装系统

- ### Phishing
- 复制一个官方网站的主页，诱使用户输入个人的机密信息，如银行账号，密码等等。
- 



实例2



Phishing的最新统计数据

- 数据来源 Symantec 2005年3月发布的互联网安全报告
- Symantec Brightmail AntiSpam™ 每周截获的phishing攻击从9百万次增长到3千3百万次

防护

- <http://www.microsoft.com/athome/security/email/phishing.mspx>
- 对特定的邮件信息要当心
- 使用XP SP2

综合保护措施

第一重要：用户培训

综合措施：

- 系统备份
- 防火墙
- 反病毒软件，反间谍软件
- 及时安装操作系统的补丁
- 尽量避免运行在系统管理员模式
- 特定的硬件配置

AutoStart工具

- 从www.sysinternals.com下载
- 检测那些程序开机自动运行

资源

Windows 安全

<http://www.microsoft.com/athome/security/spvware/default.mspx>

Rootkit

<http://research.microsoft.com/rootkit/>

Phishing

<http://www.microsoft.com/athome/security/email/phishing.mspx>

Sysinternal

<http://www.sysinternals.com>

信息安全Blog

http://blogs.itecn.net/blogs/chengyun_chu



欢迎大家的反馈!