近期病毒案例分析及清华校园网病毒防范介绍

郑先伟

CCERT

电子邮件：　zxw@tsinghua.edu.cn

电　　话：　010－62784301

近期病毒案例分析

主要以磁碟机变种病毒为例

1. 导致近期校园网ARP欺骗肆虐的元凶
2. 多种传播手段
3. 更完善的自我保护功能
4. 高可重复感染性

磁碟机变种病毒

2月27日第一次发现在清华校内某系内部网络发作，现象：

- 网络时段时续，访问外网速度慢
- 打开任何网页都可能弹出各类假冒的QQ广告信息
- 局域网内发现有大量ARP欺骗存在

检查后发现，一个局域网内有8台主机在同时进行ARP欺骗. 到某台主机上采集样本进行分析发现，杀毒软件仅能查杀样本中的部分病毒，还有大部分病毒杀毒软件无法正常查杀.

磁碟机变种病毒

经过分析病毒样本发现该病毒采用了多种新的技术.基本上包含了目前木马病毒发展的主要特征:

- 传播途径多
- 生存能力强
- 重复感染率高,变种更新迅速
- 功能齐全

磁碟机变种病毒

传播途径多样化:

- 通过网页浏览进行传播---主要的传播手段之一,利用大量可通过IE浏览器利用的漏洞进行传播,除windows自身的漏洞外,越来越多的第三方插件的漏洞被利用,如flash、realplay、pdf浏览器等。

- 通过移动存储介质传播---windows的自动播放功能进行传播，病毒感染系统后会自动恢复系统的自动播放功能，便于它有效的传播。

磁碟机变种病毒

传播途径多样化:

- 通过感染系统的EXE文件进行传播---病毒感染系统上除windows系统目录外的所有EXE文件，并对执行文件进行加壳（加密）以避免被杀毒软件查杀。病毒还会感染压缩文件，它会自动解压压缩文件感染里面的可执行文件后再重新压缩成压缩包。

磁碟机变种病毒

传播途径多样化:

- 通过ARP欺骗网页劫持传播---病毒劫持局域网内所有的网页访问，并在网页中插入带有木马链接的网页，这就使得用户访问网页的危险系数增高。

- 通过木马下载器下载---病毒感染系统后会通过木马下载器下载很多其他的木马到系统上运行，而同样其他木马感染系统后也会自动下载该木马病毒到系统上运行。

磁碟机变种病毒

生存能力强，通过多种手段反查杀:

1. 注册全局HOOK，扫描包含有常用安全软件关键字（关键字设置的很短）的程序窗口，发送大量消息，致使安全软件崩溃。通过监测系统进程中的敏感程序名来自动关闭相关的安全软件。
2. 通过系统延迟重启的方式在C盘生成高优先级的底层驱动程序并在系统启动时加载，这个驱动会检测系统上的病毒程序是否工作正常，同时卸载其他安全软件在系统中的驱动。完成上述工作后该驱动程序会被病毒删除。

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\BackupRestore\KeysNotToRestore下的

Pending RenameOperations字串（创建延迟重启的项目）

磁碟机变种病毒

生存能力强，通过多种手段反查杀:

3. 监视并修改注册表，关闭查看系统隐藏文件功能，使得用户无法看到病毒文件。

4. 监视并修改注册表，破坏系统安全模式功能，使得进入安全模式后系统会出现蓝屏错误。

5. 监视并修改注册表，令系统中的安全组策略无法正常启用。

6. 删除注册表中的所有自动启动项，以防止安全软件随系统自动启动

磁碟机变种病毒

生存能力强，通过多种手段反查杀:

7. 监视并删除注册表里面的Image File Execution Options项和子键，以防止用户通过镜像劫持来阻止病毒运行。

8. 延时启动功能，病毒感染系统后并不会马上运行，而是会休眠一段时间后再开始运行。

9. 两个病毒进程互相监视，一旦其中一个被终止，另一个会马上启动它，如果发现程序启动受阻，系统会被自动重起。

磁碟机变种病毒

多种方式导致重复感染率高:

1. 在各磁盘分区中创建autorun.inf和pagefile.pif，使得用户只要双击系统中的盘符就会被感染 .

2. 感染执行文件并对文件程序进行加壳,如果想要强行对文件进行杀毒会导致程序无法正常使用.

3. ARP欺骗网页劫持

4. 其他木马自动下载

磁碟机变种病毒

变种更新迅速:

病毒会通过网络进行自我升级(两到三天一个变种),并且更新服务器的地址也定期改变.

目前已知病毒用来升级的主服务器居然是使用千兆光纤直接接入到网络上的.

磁碟机变种病毒

功能多样化:

- 已经采用模块化设计,各功能相互独立.
- 多种木马病毒的复合体,表现形式多样,彻底查杀困难.
- 需要新的功能可以实时通过网络下载.

新病毒带来的挑战

给校园网运行带来的挑战?

1. 传统防御办法的失效(防火墙、IDS等)
2. 杀毒软件始终处于被动状态
3. 表现形式不固定
4. 网络层可控的因素变小
5. 用户端风险和操作难度增大

清华校园网病毒防范

三方面的工作：

1. 局域网部署监测设备
2. 统一部署的防病毒软件
3. 用户的安全培训

清华校园网病毒防范

03年开始陆续在学生宿舍区开始部署入侵检测设备，目前大部分的学生宿舍的子网内都有流量监听分析设备。

- 在对早期病毒的控制上效果还不错（如nachi病毒等）
- 对ARP欺骗病毒的监听效果不是很明显
- 对现在各类木马病毒控制的效果也不是很明显

清华校园网病毒防范

统一购买的杀毒软件，04年开始选型，考虑因素：

1. 能够集中控制，统一部署（网络版）
2. 能够支持校内升级
3. 中文支持好（国内有研发部）
4. 带客户端防火墙
5. 占用系统资源较少
6. 查杀率高
7. 价格便宜

当时满足条件有三家：诺顿、趋势、瑞星

最后综合性价比选择 趋势网络版防毒软件

清华校园网病毒防范

杀毒软件的使用情况:

- 教职工用户使用率较高
- 学生使用率一般

多元化的选择是否新的出路?

清华校园网病毒防范

用户的安全培训:

- 及时的安全通告（快速的应急处理）
- 针对普通用户的定期安全意识培训
- 针对特定用户的专题安全培训（办公人员、网管等）

个人用户的安全意识及操作规范在未来的防病毒工作中所占的分量越来越重!

总结

未来校园网防病毒工作发展的一些想法:

1. 多元化的控制（多种方式的结合）
2. 防范比控制更为有效
3. 终端用户的参与度越来越高


谢谢!