病毒命名

很多时候大家已经用杀毒软件查出了自己的机子中了例如

Backdoor.RmtBomb.12 、Trojan.Win32.SendIP.15 等等这些一串英文还带数字的病毒名，这时有些人就懵了，那么长一串的名字，我怎么知道是什么病毒啊？ 其实只要我们掌握一些病毒的命名规则，我们就能通过杀毒软件的报告中出现的病毒名来判断该病毒的一些公有的特性了。

世界上那么多的病毒，反病毒公司为了方便管理，他们会按照病毒的特性，将病毒进行分类命名。虽然每个反病毒公司的命名规则都不太一样，但大体都是采用一个统一的命名方法来命名的。一般格式为：<病毒前缀>.<病毒名>.<病毒后缀> 。

病毒前缀是指一个病毒的种类，他是用来区别病毒的种族分类的。不同的种类的病毒，其前缀也是不同的。比如我们常见的木马病毒的前缀 Trojan ，蠕虫病毒的前缀是 Worm 等等还有其他的。

病毒名是指一个病毒的家族特征，是用来区别和标识病毒家族的，如以前著名的 CIH 病毒的家族名都是统一的 “ CIH ” ，还有近期闹得正欢的振荡波蠕虫病毒的家族名是 “ Sasser ” 。

病毒后缀是指一个病毒的变种特征，是用来区别具体某个家族病毒的某个变种的。一般都采用英文中的 26 个字母来表示，如 Worm.Sasser.b 就是指 振荡波蠕虫病毒的变种 B，因此一般称为 “振荡波 B 变种” 或者 “振荡波变种 B” 。如果该病毒变种非常多（也表明该病毒生命力顽强 ^_^），可以采用数字与字母混合表示变种标识。

综上所述，一个病毒的前缀对我们快速的判断该病毒属于哪种类型的病毒是有非常大的帮助的。通过判断病毒的类型 ,就可以对这个病毒有个大概的评估(当然这需要积累一些常见病毒类型的相关知识，这不在本文讨论范围)。而通过病毒名我们可以利用查找资料等方式进一步了解该病毒的详细特征。病毒后缀能让我们知道现在在你机子里呆着的病毒是哪个变种。