常见病毒攻击摘要

一、Virut僵尸网络

Virut感染性病毒，是通过感染全盘可执行文件、HTML文档来达到破坏计算机系统的目的。一般是将恶意代码注入到其它进程中运行的，可以是系统进程或者其它应用进程，注入比较多的进程是系统进程winlogon.exe。感染主机的绝大多数进程都被挂了类型为inline的进程钩子，持续关注关键系统调用，截取或篡改系统信息

Virut的目的在于长期利用受害者主机，窃取用户重要信息，下载并给用户安装不必要的流氓或恶意软件，以赚取软件安装费用，也可做为DDoS终端、发垃圾或钓鱼邮件、成为跳板做欺诈等违法行为。实际上，感染Virut已经意味着主机处于重度高风险之中。

主要推荐以下几种方式进行预防与查杀：

1、使用EDR在感染病毒的电脑上进行全盘扫描查杀，查杀结束后重启计算机，并检查重启后是否有其他新的文件或进程生成。
2、Virut是感染型的顽固病毒，建议使用专杀工具进行查杀，这里推荐下卡巴斯基的Virut专杀工具。最后，由于Virut的高恶意，高传染性，仍然建议再配合使用杀毒软件进行一次全盘查杀。常见的杀毒软件很多，这里推荐下火绒的：<http://www.huorong.cn/>
注：使用其它常见杀毒软件也可，问题不大，建议多使用几个。
3、Virut病毒的变种是非常多的，黑客与时俱进，不断的加强和完善该病毒的各项能力。是否还有些不为人知的特殊技能，轻松躲过专杀工具，还不得而知。
而且Virut病毒感染的文件非常多，杀毒工具或专杀工具能否彻底查杀并修复干净，仍有一定的可能性。如果对主机的安全风险有更高的要求，建议只把文档文件复制出来（不包括html文件，所有的二进制文件也抛弃不要），然后重装系统，这样要来得更安全些。

二、Ramnit蠕虫

Ramnit 是一个典型的VBScript蠕虫病毒，能够通过网页挂马的方式进行传播，用户在浏览器中浏览挂载该恶意代码的HTML页面后并点击加载ActiveX控件后主机就有可能受到恶意代码的感染。

Ramnit病毒可以监控网络访问活动等，可能导致网上银行交易等信息泄露或盗取；该病毒还可以扫描和浏览服务器中文件系统，获取敏感的文件信息；此外该病毒通过控制某台计算机可以作为攻击者的跳板对整个内部网络造成危害。

主要推荐以下几种方式进行预防与查杀：

1、使用EDR在感染病毒的电脑上进行全盘扫描查杀，查杀结束后重启计算机，并检查重启后是否有其他新的文件或进程生成。
2、使用专杀工具，Ramnit是感染型的顽固病毒，建议使用专杀工具进行查杀，这里推荐下卡巴斯基。由于Ramnit的高恶意，高传染性，仍然建议再配合使用杀毒软件进行一次全盘查杀。
3、IE浏览器用户设置安全设置，是否执行来源不明的ActiveX控件由我们做出选择，或禁止执行来源不明的ActiveX控件。最后，我们推荐舍弃旧版本IE浏览器，使用谷歌浏览器、火狐浏览器、QQ浏览器等，都比低版本的IE强
查看详情：
<http://bbs.sangfor.com.cn/forum.php?mod=viewthread&tid=28029>
EDR杀毒工具：
<http://edr.sangfor.com.cn/tool/SfabAntiBot.zip>
专业杀毒软件：
<http://edr.sangfor.com.cn/tool/FxRamnit.exe>