火绒安全
HUORONG SECURITY

火绒安全解决方案

威胁、挑战和机遇

2021/08/30

公　　司：北京火绒网络科技有限公司

地　　址：北京市朝阳区红军营南路 15 号瑞普大厦 D 座 4 层

网　　址：https://www.huorong.cn

电　　话：400-998-3555

版权声明

目录

用户面临的威胁

终端用户是火绒安全软件的服务对象，所以要保护终端用户的系统安全，首先我们需要分析终端用户真正面临的威胁是什么。

恶意软件

恶意软件（Malware）是指包括木马、后门、蠕虫、感染型病毒等在内的各种包含恶意代码文件的统称。由于早期的恶意软件基本都属于感染型病毒，所以通常我们也将恶意软件统称为病毒。

从 2007 年左右开始，得益于互联网的快速普及，恶意软件数量呈现快速增长的趋势。传播方式也从之前的文件感染、局域网传播等传统方式迅速转变为通过社工、挂马等互联网化的传播方式。早期常被应用于感染型病毒的代码多态、变形技术被应用于恶意软件生成器、混淆器等，恶意软件作者通过混淆器不断快速迭代生成新恶意样本，以此来对抗安全软件的查杀。

灰色软件

灰色软件一般指广告类（Adware）程序，这类程序往往会通过弹出广告等方式诱导、欺骗甚至是恐吓用户以达到推广获利的目的。这类程序不属于一般意义上安全行业内对恶意软件的定义，但却对用户正常使用电脑产生极坏的影响。

基于上述原因，不同安全软件也采取了不同的策略来进行应对，多数安全软件会把此类程序识别为广告程序（Adware），或潜在不受欢迎程序(Potentially Unwanted Application，即 PUA)，或类似卡巴斯基检出的病毒名以 not-a-virus:开头的威胁。

软件侵权

软件的诱导/恐吓/静默推广、捆绑安装、流量劫持、非功能性的隐私数据收集、无法禁用的广告推送等等，均属于软件侵权的行为。

近年来，在互联网变现的高额利益诱惑下，越来越多的“正常软件”通过各种侵权行为把用户的电脑作为“肉鸡”进行操纵从而获利。法律监管的空白、职业操守的缺失，使得甚至一些安全软件自身也存在诸多软件侵权行为，这些监守自盗的“保安”甚至比单纯的“强盗”更加可怕。

不良网络内容

在互联网的世界中，从来不缺少投机者。挂马网站、仿冒网站、欺诈网站、非法网站等不良网络内容始终威胁着用户的网络安全。落入仿冒网站付款导致资金损失的案例屡见不鲜。这些网站往往具有很强的欺骗性和隐蔽性，非专业安全从业人员很难发现其中的门道。

安全软件面临的挑战

安全软件与安全威胁间的较量正书写着整个安全行业的历史，而本节所讨论的内容仅聚焦在 2007 年以后，即互联网时代的安全挑战。

技术对抗

技术对抗的手段多种多样，这里只列举较为显著的几类：

1、混淆类样本数量暴增

2007 年可谓是混淆技术的分水岭，以 Trojan/C2Lop（业内通常称其外层混淆器为 Swizzor）为代表的各种自定义壳和混淆样本大量涌现。以高级语言作为外层包裹器（Wrapper）的样本更是不胜枚举，传统安全软件的脱壳、解码技术受到了巨大的挑战，脚本虚拟机、通用脱壳（Generic Unpacking）等技术开始应运而生并备受关注；

2、恶意软件快速迭代

随着互联网的发展，“云”的概念被应用于安全软件，安全软件对恶意软件问题的响应速度大大提高。然而，互联网的发展不仅仅造就了“云”，黑色、灰色软件利益链条也得到快速完善。在这个完善的生态系统中，每个角色都发挥着各自的“技术优势”，黑站挂马、恶意软件制造、恶意代码混淆、流量联盟分工合作。恶意软件背靠着这个庞大的生态系统快速迭代，对安全软件带来了巨大的挑战；

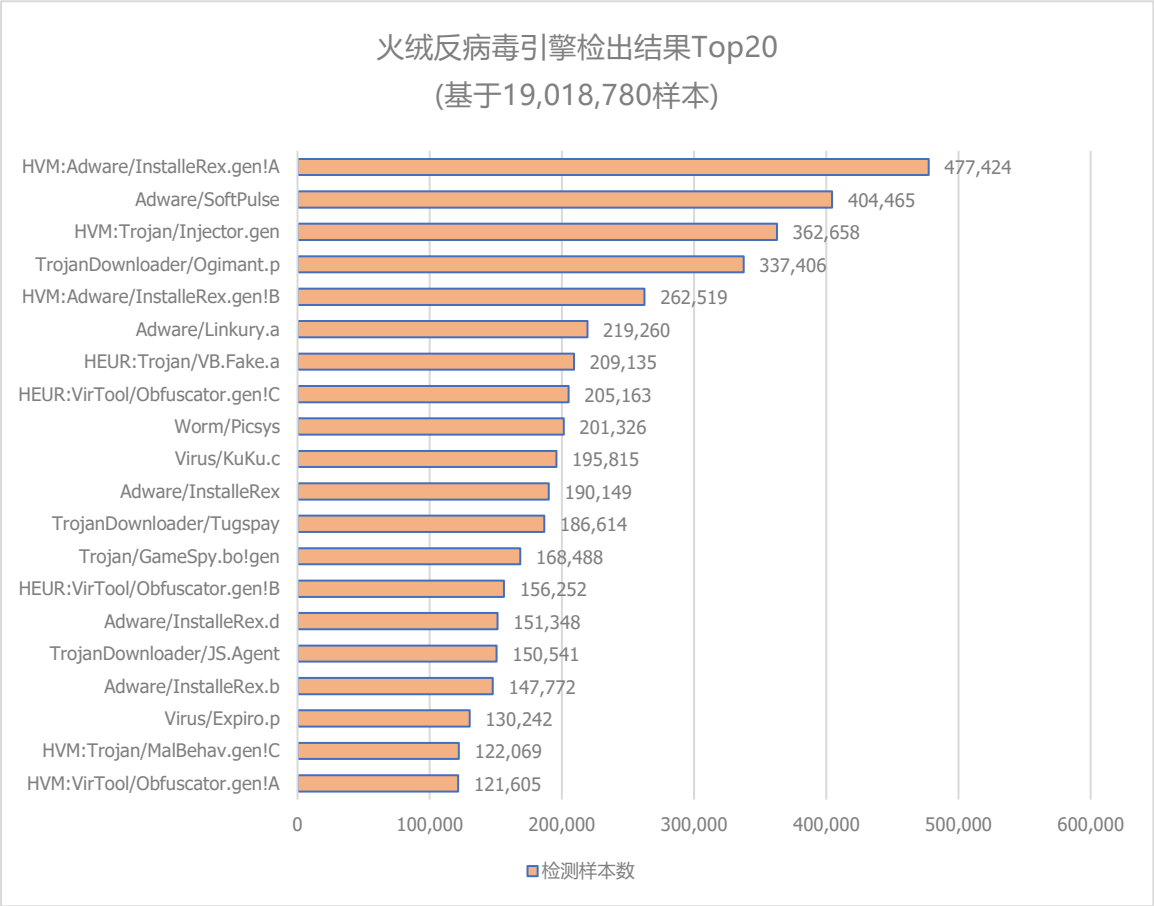
3、攻击手段多元化

攻击手段的多元化也是近些年来安全软件面临的挑战之一。信任利用（即通常说的白加黑）、高持续性威胁（APT）、分级渗透等，攻击的手段也颇具隐蔽性。传统的基于进程信任的单步、多步防御系统均成为此类威胁的“打击目标”。从火绒

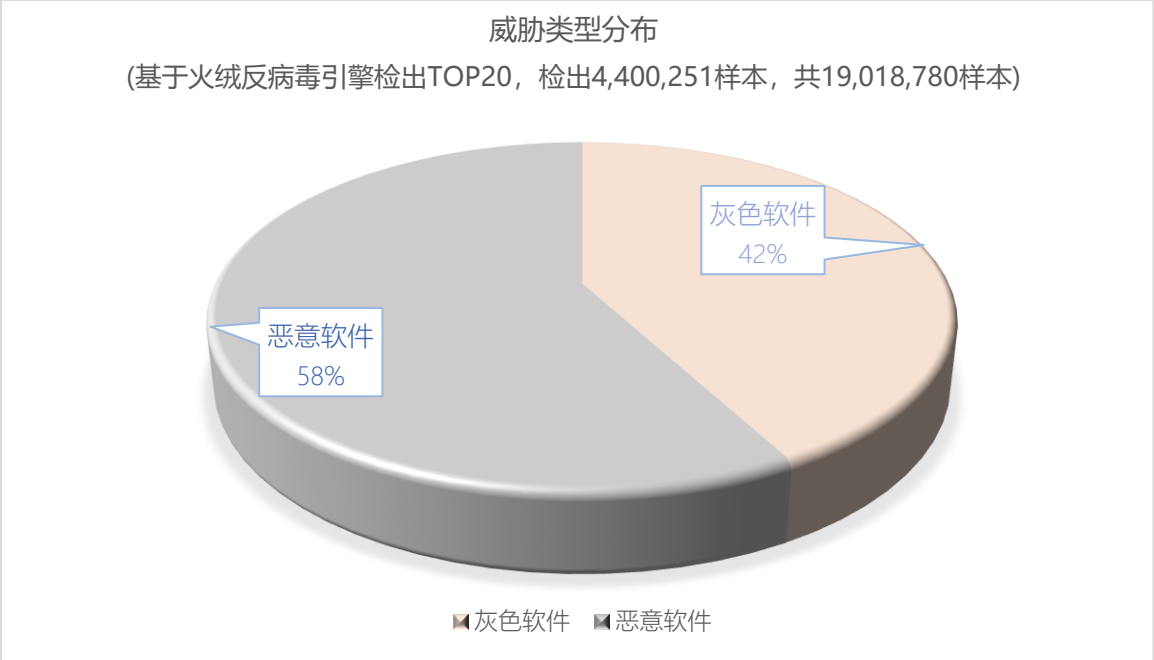
这几年实践的经验来看，基于行为分析的多步防御体系对于此类威胁具有较强的应对能力；

威胁转型

下面的图表展示的是火绒反病毒引擎在超过 1900 万样本集合的检出结果 TOP20，其中每一个柱状表示的是一条特征检出的样本数。前 20 个特征共检出了超过 400 万样本。



从上图的病毒名可以看到广告类灰色软件（Adware）占据了较大的比例。通过分别累加上图中灰色软件和恶意软件的检出数量，可以得到以下数据：



可见，前 20 位检出的样本中 42%为广告类灰色软件，可见灰色软件的比例在全部威胁类型中比例是相当巨大的。

由于灰色软件不像传统恶意软件具有典型的恶意行为，往往不同的厂家均有不尽相同的评估标准，所以为安全软件带来了一定的挑战。然而，通常这些挑战并不是来自技术层面，而更多的是来自法律和社会层面。

另外，近 2 年来，随着移动端的普及，移动端恶意代码的数量也有着较为明显的上升趋势。

火绒安全解决方案

分层防御架构

通过对各种威胁类型以及恶意软件与安全软件对抗手段的分析，可以很明显地看出，单一的技术手段不足以在当今的威胁战争中赢得胜利，只有综合多种防御技术的解决方案才能在如此复杂多变的威胁环境中胜出。

火绒安全解决方案贯彻了综合防御的理念，通过组合多种防御技术，自上而下地在所有可能的威胁入口设计了独特的防御策略，共同有效地防御不同类型的恶意威胁。下图为火绒安全解决方案的分层防御架构：

内容拦截层

代码以文件形式进入用户电脑，首先会被内容拦截层进行扫描，如扫描到威胁则阻断用户对该恶意威胁的触碰并根据需要进行隔离操作。该层对应火绒安全软件以下功能：

1. 文件实时监控

- 防御重点：恶意软件、灰色软件；
- 功能定义：当文件被执行、修改、访问时，文件实时监控通过火绒反病毒引擎对相应文件进行扫描。用户可以根据自己需求配置不同的扫描策略，包括扫描时机和反病毒引擎相关配置等；

2. 下载保护

- 防御重点：恶意软件、灰色软件；
- 功能定义：与文件实时监控类似，当浏览器、下载工具或即时聊天软件下载或接收文件时，下载保护功能会通过火绒反病毒引擎对相应文件进行扫描。下载保护的意义在于，当文件实时监控功能处于只监控文件执行状态时，仍然可以在通过流量入口获取文件后第一时间对文件进行病毒扫描；

3. U 盘保护

- 防御重点：恶意软件、灰色软件；
- 功能定义：当 U 盘接入时，通过火绒反病毒引擎主动对 U 盘中的文件进行扫描。同时，针对隐藏文件等 U 盘传播类恶意软件常见恶意修改操作进行修复；

4. 软件安装拦截

- 防御重点：软件侵权；
- 功能定义：当程序执行时，软件安装拦截模块会通过火绒反病毒引擎对程序文件进行分析，如果识别为软件安装则征求用户是否允许该软件的安装请求，还用户自主选择软件安装的权利，杜绝静默捆绑类安装；

5. 邮件监控

- 防御重点：恶意软件；

- 功能定义：当通过邮件协议收发邮件时，邮件监控模块会通过火绒反病毒引擎对相应邮件内容进行扫描。用户可以根据自己需求配置不同的扫描策略，包括扫描范围以及邮件协议等；

6. Web 扫描

- 防御重点：恶意软件；
- 功能定义：当通过 HTTP 协议接收到对 URL 的请求内容时，Web 扫描模块会通过火绒反病毒引擎对接收到的数据内容进行扫描。改功能不仅可以更早检测到恶意代码并且可以追溯到恶意代码来源（URL），为溯源分析提供了良好的支持；

规则拦截层

若内容拦截层没有检测到威胁，那么当程序被执行时，规则拦截层开始生效，并根据基础防护或自定义防护规则，对程序产生的违例动作进行拦截。这就是通常所说的单步防御。该层对应火绒安全软件以下功能：

1. 系统加固（文件保护、注册表保护、进程保护）

- 防御重点：恶意软件、软件侵权；
- 功能定义：保护操作系统文件、注册表、进程等资源不被非法篡改，火绒基础防护规则针对不同类型的资源进行了逻辑分组，用户可以有针对性地进行选择；

2. 执行控制

- 防御重点：恶意软件、灰色软件；

- 功能定义：当程序执行时，执行控制会判断本次执行操作是否符合基础防护规则预定义的行为抽象，例如通过命令行创建、删除用户账户等。如果符合，则会向用户征求处理方式；

3. 危险动作拦截
   - 防御重点：恶意软件、灰色软件、软件侵权；
   - 功能定义：监控可能对系统产生潜在风险的动作，如加载驱动、写磁盘保留扇区等，当动作产生时，根据功能设置选择阻断或征求用户。该功能的意义既在于阻断恶意软件对系统产生的潜在风险，也可以从灰色软件、正常软件中剥离潜在的非必要或侵权功能；
4. 病毒免疫
   - 防御重点：恶意软件；
   - 功能定义：以规则的形式对恶意软件典型感染路径进行免疫，避免恶意软件对系统的感染；
5. 联网控制
   - 防御重点：恶意软件、灰色软件、软件侵权；
   - 功能定义：细粒度控制程序的联网行为，可以在 TCP 层控制程序的出站和入站行为，并可以分别限制程序的上传和下载速率；
6. IP 协议控制
   - 防御重点：恶意软件、灰色软件、软件侵权；
   - 功能定义：以规则的形式控制 IP 层出站和入站的数据流量；
7. 自定义防护规则
   - 防御重点：恶意软件、灰色软件、软件侵权、不良网络内容；

- 功能定义：允许用户自定义文件、注册表防护规则，以及网址拦截规则，方便用户有针对性地对敏感数据进行保护，或对特定网址进行拦截；

8. 应用加固
   - 防御重点：黑客攻击；
   - 功能定义：通过约束应用软件的动作和行为，防止应用软件被黑客利用潜在漏洞对终端进行攻击；
9. 摄像头防护
   - 防御重点：隐私安全；
   - 功能定义：防止用户摄像头在未经用户许可的情况下被打开，保护用户的隐私安全；

行为拦截层

在程序运行时，程序的每个动作都会被行为拦截层所捕获。行为拦截层会对捕获到的动作进行关联和抽象，产生进程、线程及行为的多维分析矩阵，并根据启发式分析逻辑判定程序的行为是否具有威胁。当发现威胁时，行为拦截层阻止威胁进程及关联进程、线程的执行，并尽可能地回滚已经产生的潜在风险。这就是通常所说的多步防御。该层对应火绒安全软件以下功能：

1. 病毒行为监控
   - 防御重点：恶意软件、灰色软件；
   - 功能定义：规则拦截层的危险动作拦截只对有潜在风险的动作进行拦截，而行为拦截层则在后台持续对程序的行为进行启发式分析。通常程序的单个动作并不足以判定是否具有潜在威胁，而多个动作和行为的组合则可能威胁系

统安全。例如，分别判断“手持水果刀”和“站在人群中”这两个动作，均不能判定存在威胁，但“手持水果刀站在人群中”这个行为就可能威胁他人安全了。行为拦截层的意义就在于此；

2. 软件安装拦截

- 防御重点：软件侵权；
- 功能定义：火绒软件安装拦截功能推出后，对静默推广类软件侵权行为起到了有效的打击作用。近一年来，越来越多静默推广安装行为采用“组件式安装”的方式，而不是通过独立安装包的方式安装。所以，火绒在 3.0 版本引入了行为启发逻辑来识别软件的安装行为；

内容过滤层

内容过滤层主要被设计用来解决网络数据包的安全威胁问题，即基于内容过滤的防火墙。该层对应火绒安全软件以下功能：

1. 恶意网站拦截

- 防御重点：不良网络内容；
- 功能定义：根据对发送 HTTP 请求内容的分析，在协议层阻断用户对木马盗号、钓鱼仿冒、虚假欺诈等各类潜在风险网站的访问；

2. 网络入侵拦截

- 防御重点：高危漏洞攻击；
- 功能定义：在 IP 层对出站和入站数据包进行分析，可在未打相应补丁的情况下检测并拦截高危漏洞攻击行为，如永恒之蓝等；

3. 横向渗透防护

- 防御重点：恶意软件、黑客攻击；
- 功能定义：通常黑客在攻破公网主机后，会通过横向渗透的手段在内网“扩大战果”，该功能在网络层解析 Windows RPC 协议检测并拦截潜在横向渗透行为；

4. 对外攻击拦截
   - 防御重点：高危漏洞攻击；
   - 功能定义：在 IP 层对出站和入站数据包进行分析并拦截终端对外发起的高危漏洞攻击行为；
5. 僵尸网络防护
   - 防御重点：恶意软件、黑客攻击；
   - 功能定义：通过对后门病毒的控制协议进行解析，检测并拦截黑客利用后门病毒对终端的远程控制行为；
6. 暴破攻击拦截
   - 防御重点：黑客攻击；
   - 功能定义：通过对网络流量进行协议分析监测并统计利用 SMB、RPC、RDP 等协议的登陆行为，检测并阻断潜在黑客对终端的暴力破解登陆行为；
7. Web 服务保护
   - 防御重点：黑客攻击；
   - 功能定义：通过对网络流量进行协议分析，检测并阻断潜在针对 IIS、Apache 等 Web 服务漏洞的攻击行为；

综上所述，火绒安全软件会在上述分层防御架构的基础上，横向扩展防御广度，并深入挖掘单个防御技术的技术实力，力求打造完善、有效的综合防御解决方案。