火绒安全
HUORONG SECURITY

火绒 2019 年 PC 端安全回顾与总结

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

前言

根据火绒安全 2019 年威胁数据统计分析，个人终端遇到的问题以恶意代码（病毒）、流氓软件问题为主。企业除以上问题外，渗透攻击类问题也越发严重。

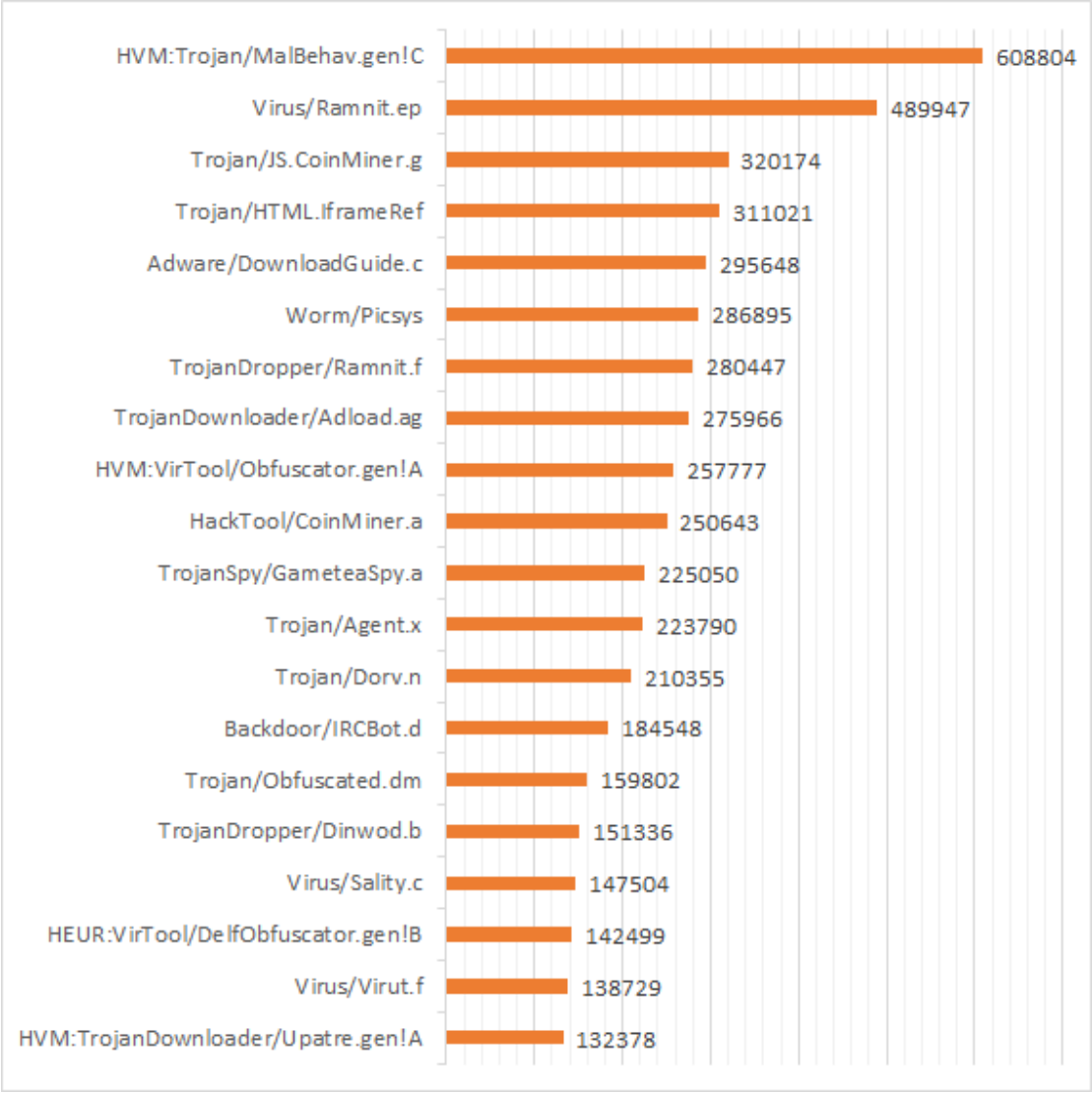
恶意代码（病毒）勒索病毒、蠕虫病毒和挖矿病毒为 PC 终端用户所遇到的主要问题。由于近年来病毒使用混淆器的情况越来越普遍，混淆器更新迭代的速度也越来越快，最终造成主要流行病毒变种的产生速度快速提升，每年所产生的样本量愈发巨大。

与具体的病毒问题不同，随着病毒传播途径的多元化，黑客渗透攻击也日渐成为了互联网中的主要安全问题之一。企业遭遇渗透攻击类问题逐渐增多，主要表现为黑客针对性的对企业网络或服务器进行入侵，盗取终端数据或使用勒索病毒加密数据文件进行勒索。黑客渗透攻击时，通常使用暴力破解、漏洞攻击、SQL 注入、社工等方式。

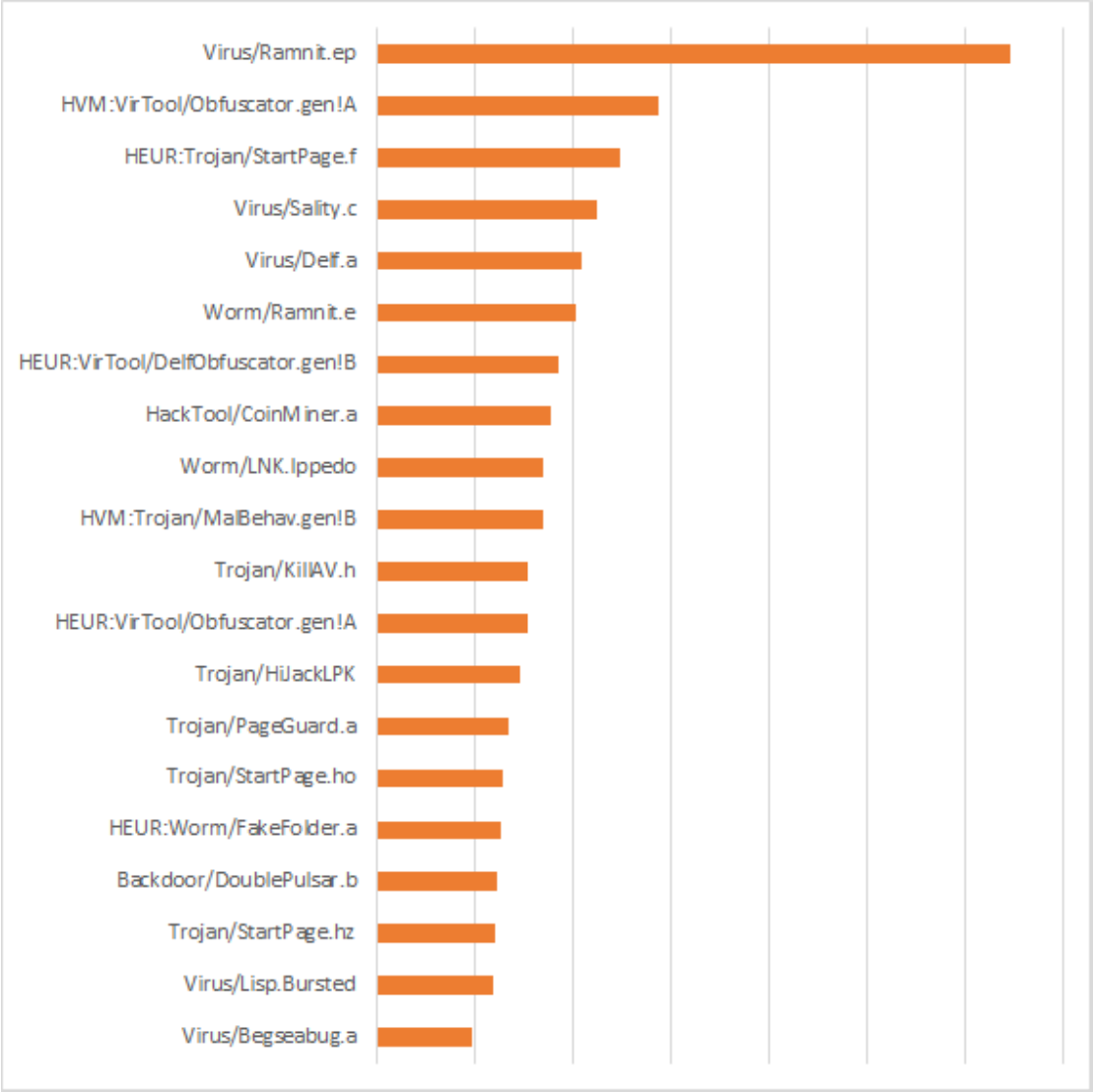
虽然黑客和病毒攻击类问题在逐渐增多，但是 2019 年对于个人用户而言，最主要的安全问题依然为流氓软件。从最早带有恶意推广代码的破解工具、激活工具，转变为通过大型商业软件通过“云”控配置操纵用户电脑收集信息、执行流氓推广逻辑。流氓软件已经不再是“盗版软件”的代名词。

恶意代码问题

2019 年，火绒安全实验室根据反病毒引擎对 2019 年全年捕获样本的检测结果，统计得出全年 Top20 流行病毒（如下图所示）。下图内数据为样本基于 HASH 去重后，仅保留不同“变种”扫描结果。



根据火绒情报威胁系统，我们对外网参与“火绒用户体验提升计划说明”感染终端对病毒检测数量的 Top20（如下图）：



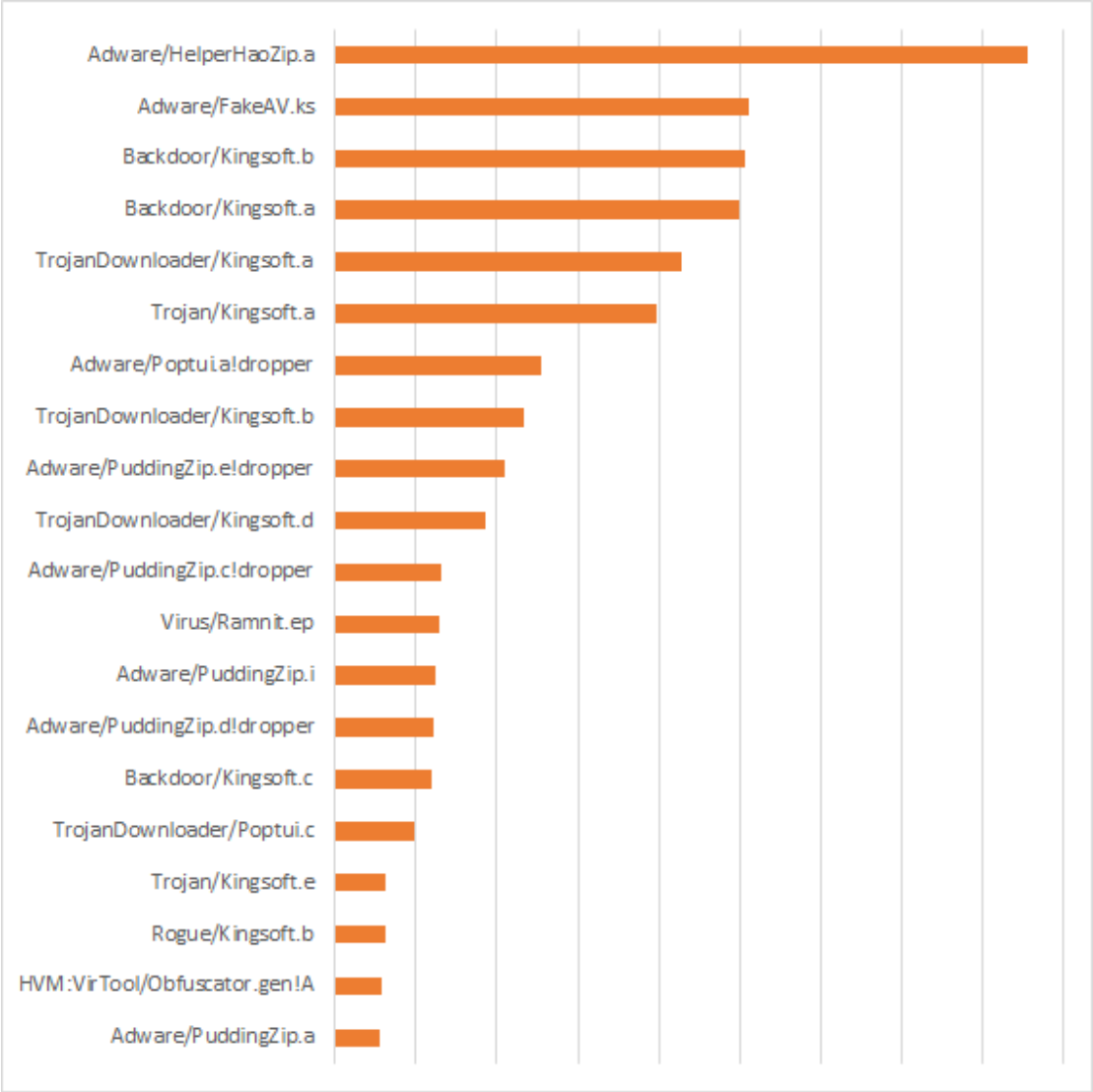
根据上图统计，使用了代码变形、反跟踪、反虚拟机等技术手段与安全软件进行技术对抗的代码混淆器（VirTool）和感染型病毒数量依然居高不下。这也是我们在个人版和企业版产品日常运营中时常遇到的问题。

火绒的日志上报和截获的样本，并不能代表“在野”样本的“绝对数量”，但是可以反映互联网中这些病毒的基本比例。长期来看，使用对抗手段的病毒会逐渐增多、病毒新变种不断迭代更新，对这些病毒的检测更需要依赖引擎方法。可以预见，在未来添加了对抗手段的病毒会逐渐增多。

流氓软件问题

从目前国内网络安全环境来说，相较于恶意代码问题而言，“流氓软件”反而是国内更为普遍的安全问题。一些大型的软件厂商为了从用户终端上牟取利益，在用户的“常用软件”中加入了流氓推广甚至恶意代码逻辑。由于这些软件已经具有一定的用户粘性甚至相当规模的用户群体，所以更是让人防不胜防。更为遗憾的是，一些用户为了继续使用这些“常用软件”功能，在得知软件带有恶意代码逻辑后无奈选择“忍痛信任”，被迫继续使用。

2019 年火绒揭露的流氓软件数量众多，但由于流氓软件与安全软件进行免杀对抗的频率较低，产生的相关样本也较少，所以在火绒截获数量最多的恶意软件列表中流氓软件并未出现。火绒监测到“在野”影响终端数量前 20 的恶意软件中，绝大多数为火绒 2019 年报出的流氓软件相关恶意软件名称（相关事件分析报告详见附录）。如下图所示：



火绒 2019 年在线技术支持问题回顾

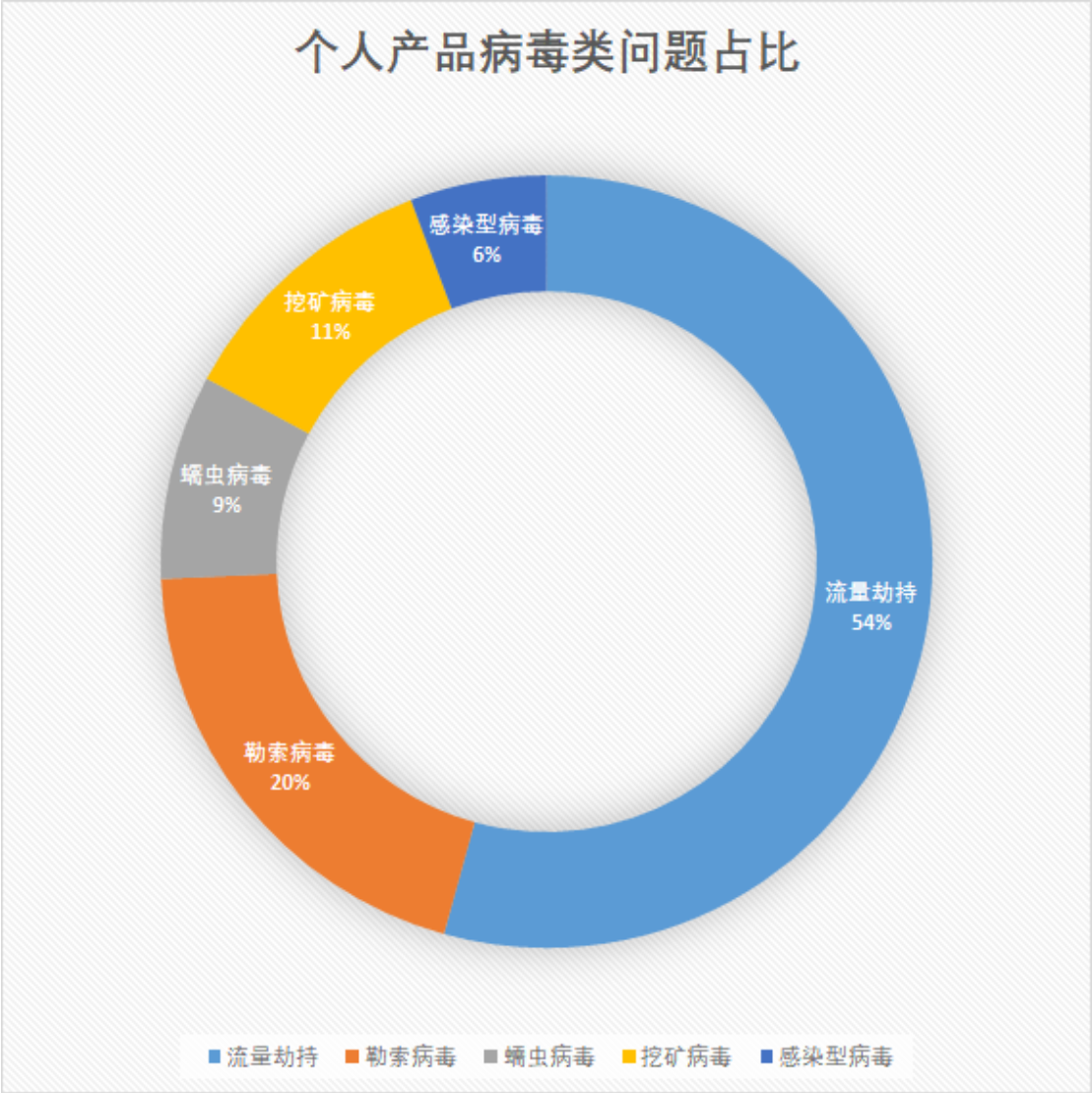
2019 年火绒为个人产品和企业产品的远程服务创建了“火绒在线支持和响应中心”。客户反馈问题后，火绒运营团队会根据用户问题为客户创建“问题档案”，记录并跟踪处理过程。

在这里需要说明的是，企业用户问题数据全部来自"火绒在线支持和响应中心"的统计，火绒企业产品不会从终端以及中心收集任何数据。

今年我们对个人用户和企业用户的分类没有基于用户自身的“属性”，而是基于用户使用火绒产品本身。在运营过程中我们发现有很多用户将个人产品用于对企业服务器的防护，所以在下面的个人产品统计中，可以看到大量勒索和挖矿病毒的数据。这里我们建议企业用户部署安全防护功能更全面的企业版产品。

个人用户主要安全问题

个人产品线遇到的病毒类问题比例如下:



对火绒个人产品用户提供的技术支持中，有超过 50%的流量劫持问题。以目前的网络环境来看，用户在安装系统、使用激活工具、下载、使用软件的过程中，都会遇到恶意推广、流氓软件、流量劫持、个人信息泄露等问题。

流量劫持类病毒

在火绒 2019 年对个人用户提供的技术支持中，流量劫持问题占全部问题的 54%，黑灰产业利用多种方式长期驻留用户电脑，通过加载恶意驱动、修改注册表、释放用户不易发现可执行程序等方式，在用户计算机内通过锁定浏览器主页、暗刷流量、窃取数据等方式获利，对用户日常使用计算机造成困扰。火绒 2019 年流量劫持类病毒相关的分析报告，见附录报告列表[1]。

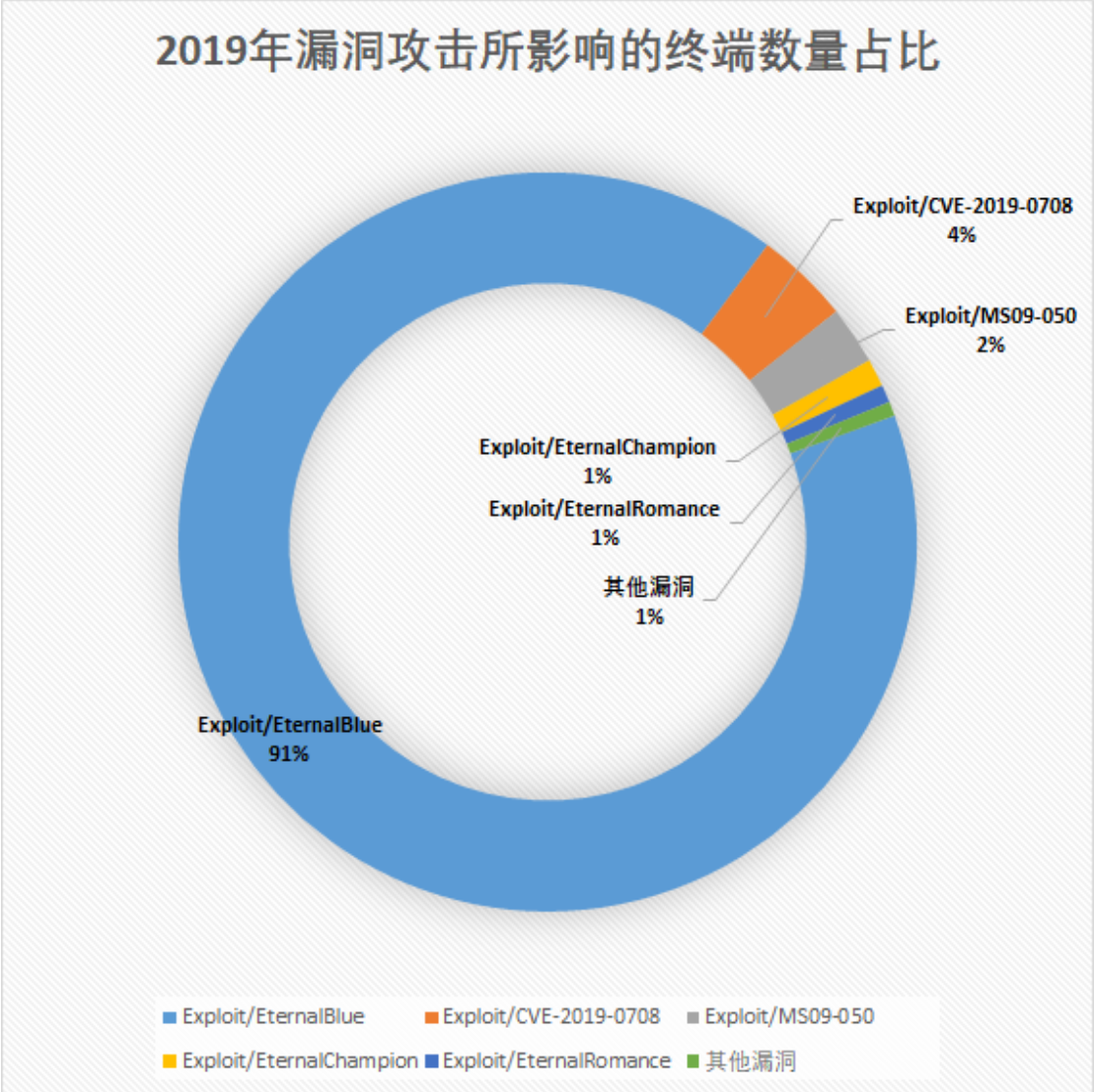
流氓软件

如前文所述，2019 年受流氓软件影响的终端数量依然较多，问题主要集中在流量劫持、广告弹窗和窃取用户隐私等方面。在火绒揭露的流氓软件中，不乏一些装机量较多、体量较大的“软件厂商”，如金山系列软件、酷我音乐等。这些软件经过多年的软件运营和用户积累，其软件功能产生了一定的用户粘性，因此在执行诸如窃取用户隐私、流量劫持等恶意行为时，则更是让用户防不胜防。火绒 2019 年流氓软件相关的分析报告，见附录报告列表[2]。

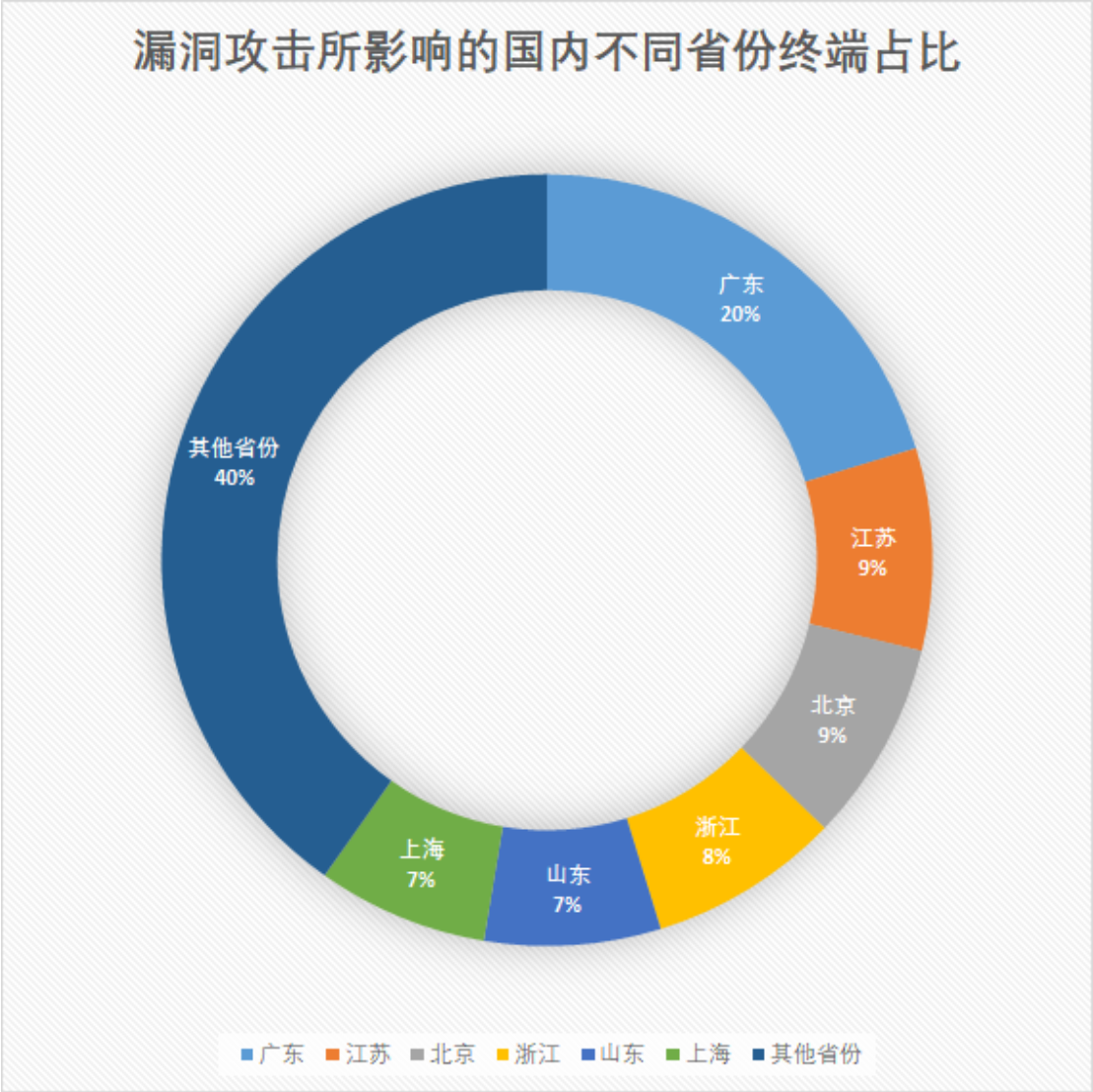
蠕虫病毒与漏洞攻击

2019 年在互联网中大肆传播的蠕虫病毒（如：WannaMine、NSABuffMiner 等）都在不同程度上使用了漏洞攻击的传播方式，致使这些病毒在互联网中的感染量较多。

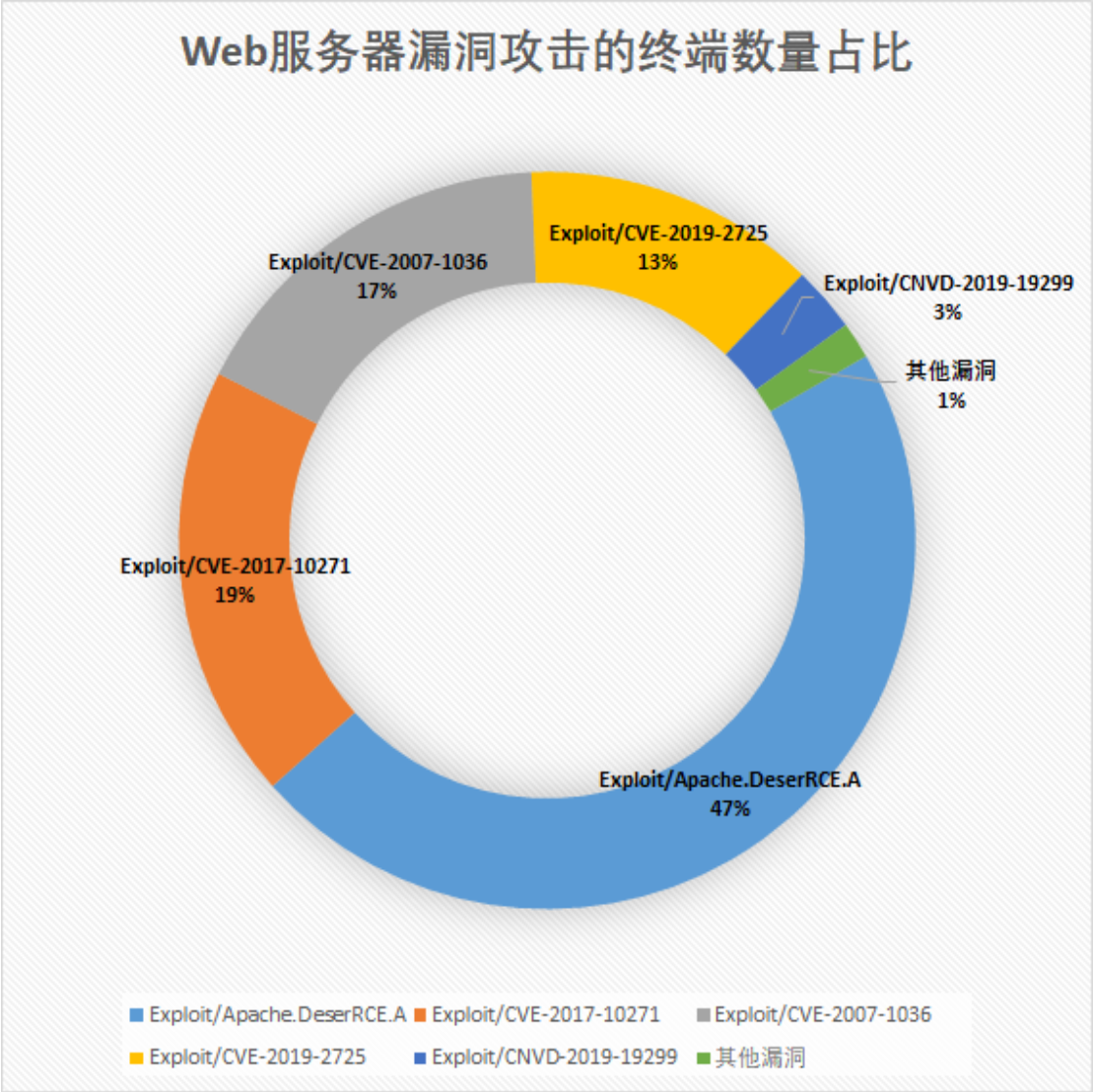
2019 年火绒监测到的蠕虫级漏洞攻击占比情况，如下图所示：



根据数据显示，“永恒”系列漏洞（Exploit/EternalBlue、Exploit/EternalChampion、Exploit/EternalRomance 和 Exploit/EternalSynergy）在黑客或病毒攻击活动中依然占据主导地位，占比约 93%。除此之外，2019 年 5 月报出的远程桌面服务漏洞 CVE-2019-0708 也在漏洞攻击总量中占有一定比例。上述漏洞攻击所影响的国内不同省份占比图，如下图所示：



除此之外，Web 服务漏洞也是恶意软件传播的主要渠道。服务器管理人员在搭建 Web 服务器时，如果使用了过于陈旧的 Web 服务软件，则都有可能遭受此类攻击。2019 年 Web 服务漏洞攻击占比情况，如下图所示：

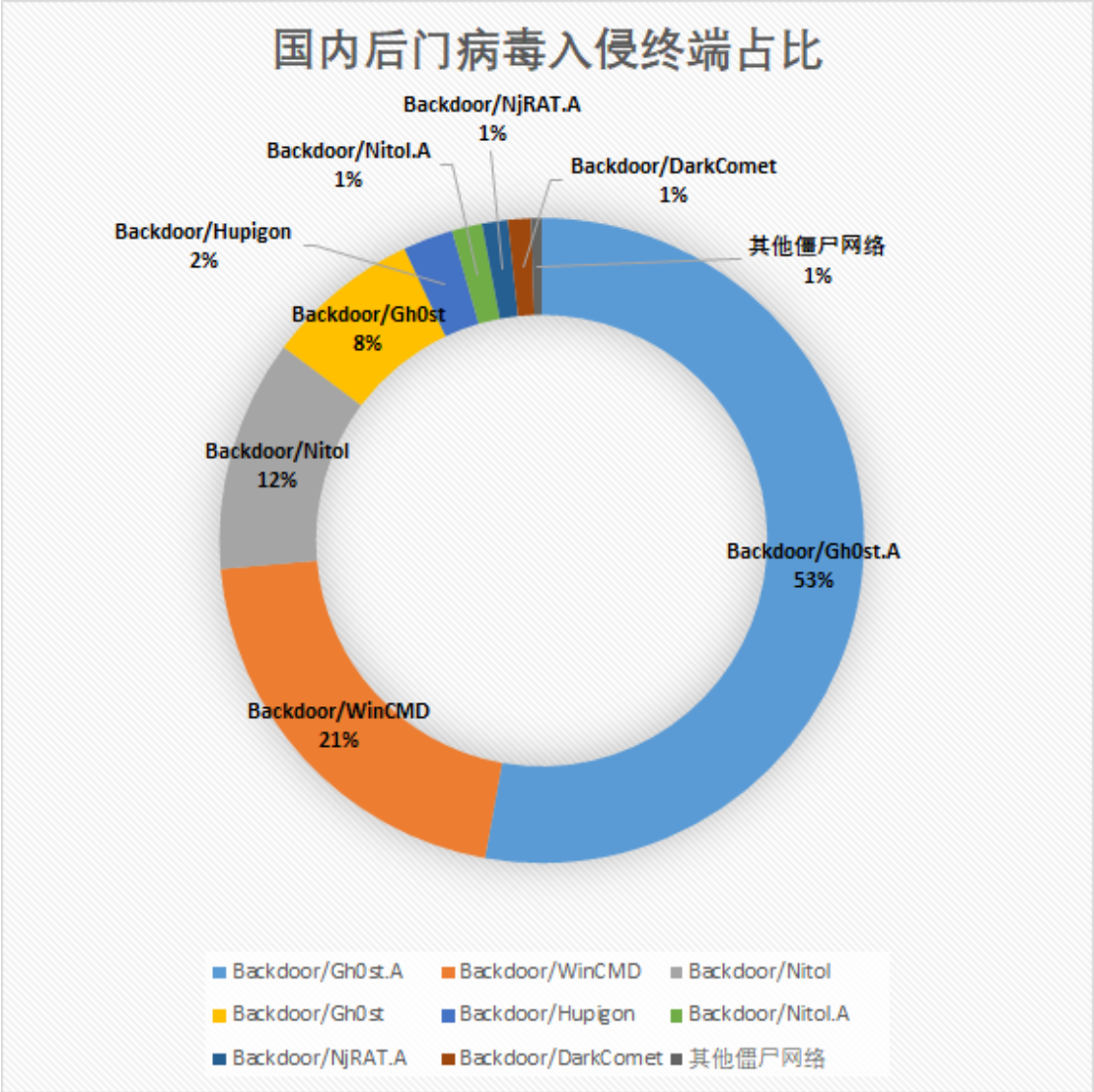


2019 年互联网中还出现过利用第三方软件的升级劫持漏洞进行病毒传播的情况，漏洞所涉及软件均为用户量较大的第三方软件，如阿里旺旺、QQ 等。这些第三方软件后续已经针对漏洞进行了紧急升级。相关报告可参见附录中报告列表[3]。

后门病毒

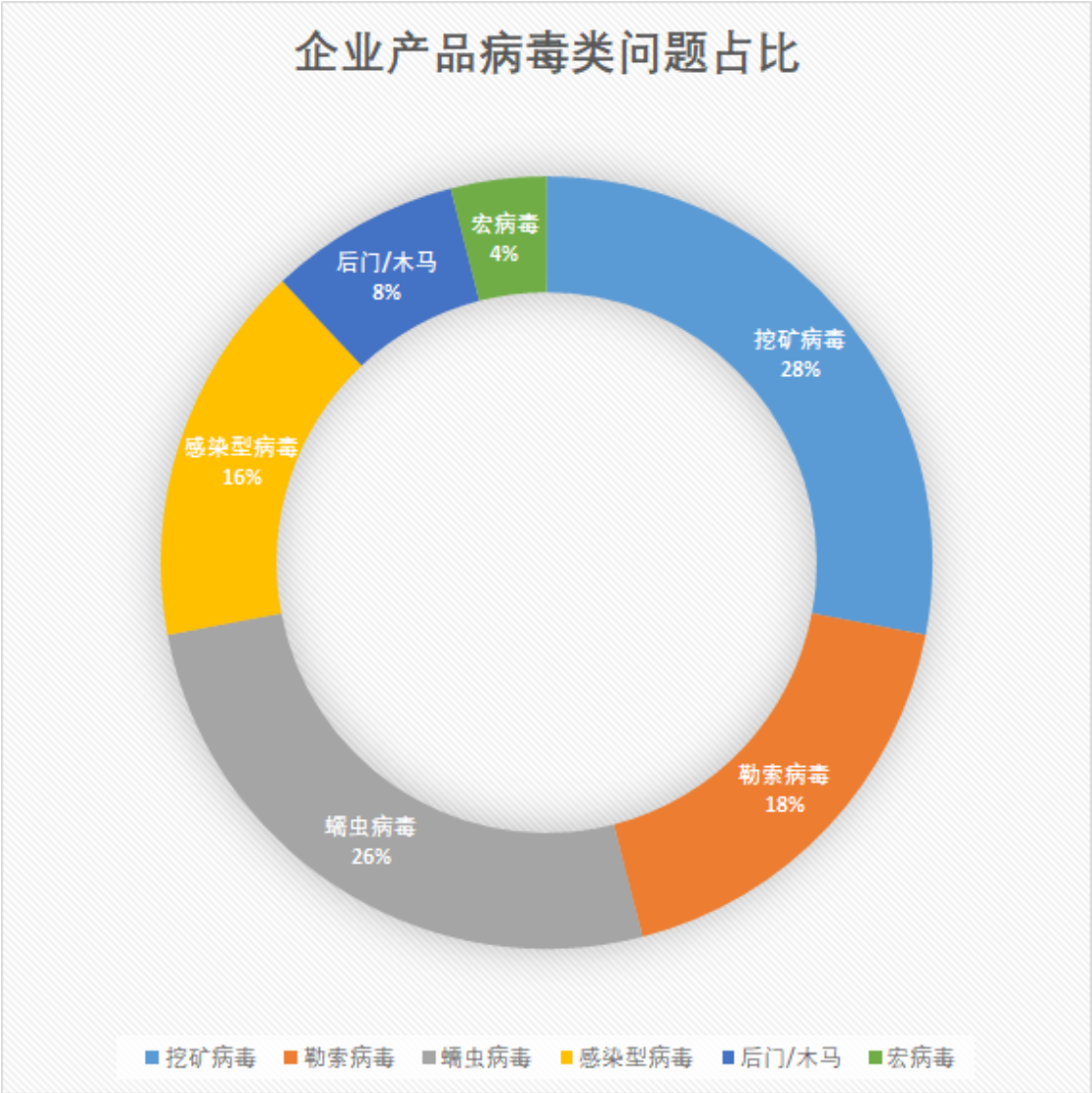
后门病毒也是 2019 年个人用户所遇到的主要安全问题之一，通过火绒检测到的防御数据统计，Gh0st 远控后门在 2019 年的僵尸网络攻击事件中占比过半。Gh0st 远控后门

最早可以追溯到 2001 年，但由于该后门相关代码已经开源，致使 Gh0st 后门变种层出不穷。国内后门病毒入侵终端占比，如下图所示：



企业用户主要安全问题

企业产品线遇到的病毒类问题比例如下:

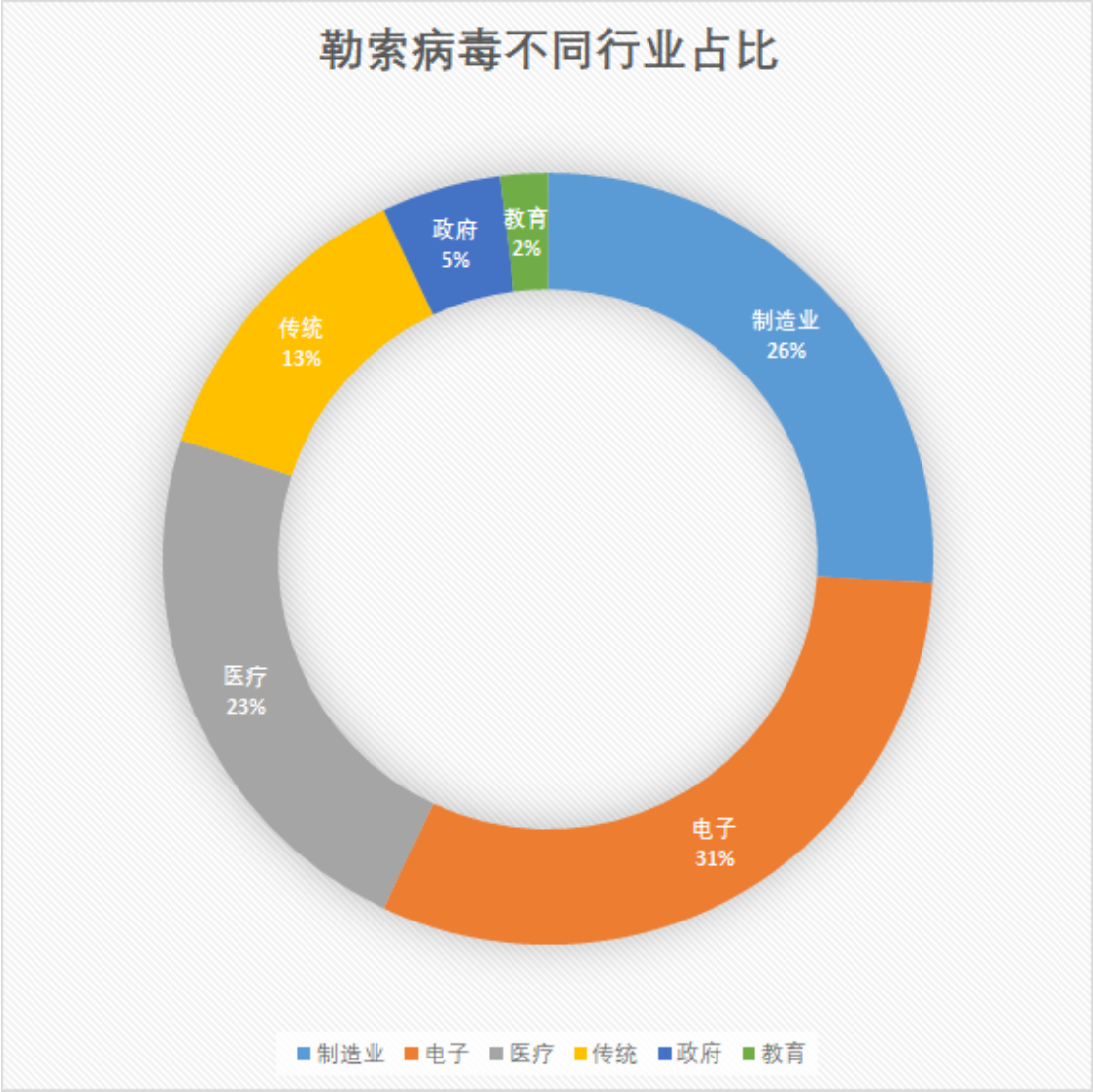


根据火绒 2019 年“火绒在线支持和响应中心”内所记录的企业服务数据，可说明火绒企业版用户常见问题与常见安全隐患，如占比较高的挖矿病毒、蠕虫病毒、勒索病毒等问题，以下内容为火绒全年内，对企业用户进行在线技术支持问题的回顾。

勒索病毒

2019 年，根据火绒"火绒在线支持和响应中心"数据显示，勒索病毒对政企的攻击逐渐增加，犯罪组织的运营方式也越发“系统化”，并且除了加密文件勒索赎金外，部分勒索病毒(例如 Maze 勒索)还增加了盗取企业数据的行为，对企业造成更大损失。

根据"火绒在线支持和响应中心"平台内数据，火绒全年对"勒索病毒"事件进行的技术支持中，电子、制造业、医疗行业遭受勒索病毒攻击最为严重。



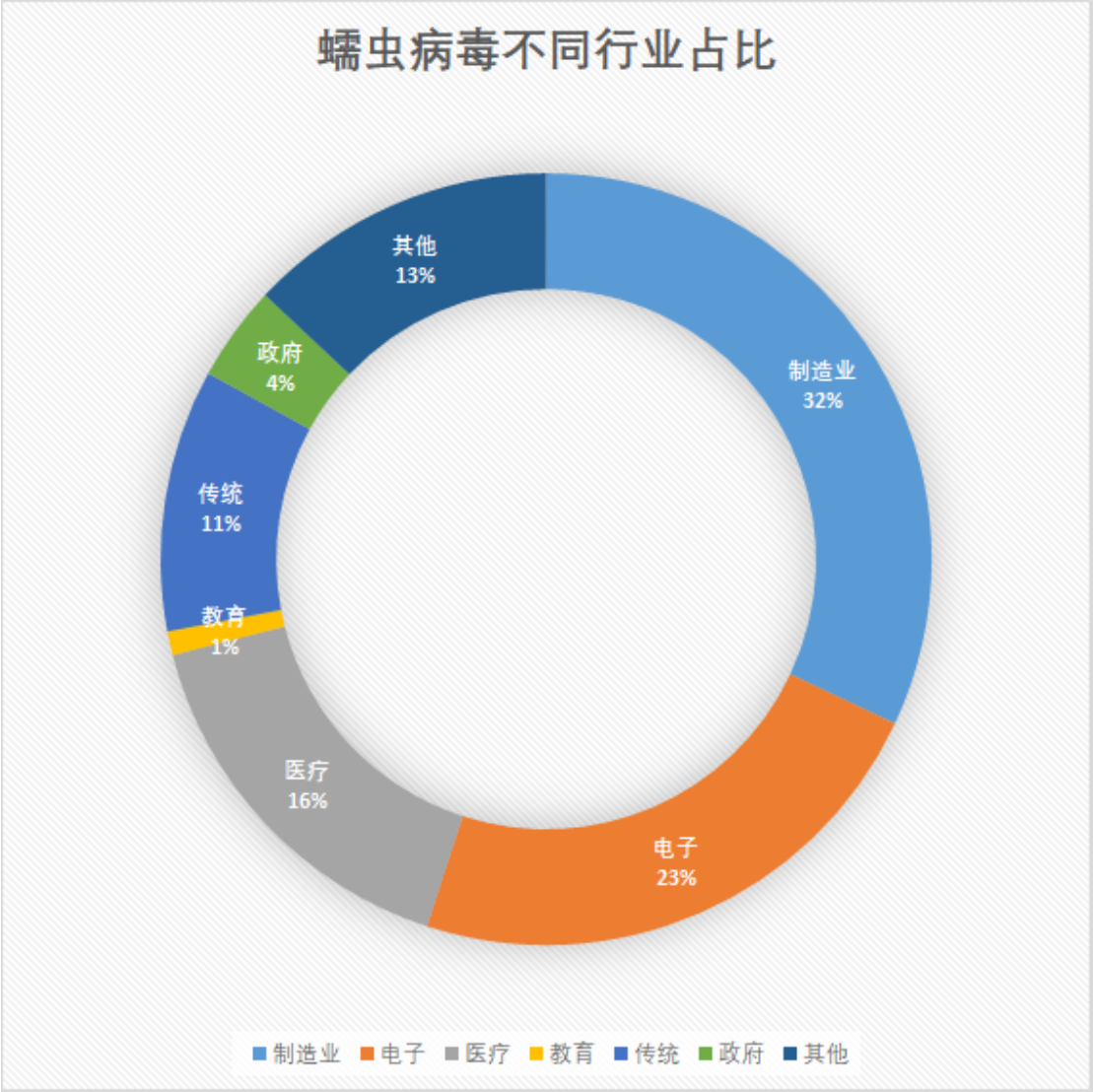
根据报告《勒索事件回顾：RDP 弱口令渗透愈演愈烈》[4]（下文中简称“勒索事件回顾”）内数据统计，黑客多选择通过 RDP 弱口令进行入侵，入侵完成后会运行勒索病毒加密文件或盗取数据。

除 RDP 弱口令外，在“勒索事件回顾”报告中，部分勒索病毒选择通过钓鱼邮件，软件捆绑，僵尸网络等方式传播，例如 RYUK 勒索病毒，通过 Trickbot 进行传播，此勒索病毒攻击成功后，会根据企业规模定制赎金，且索要的赎金金额较为巨大。

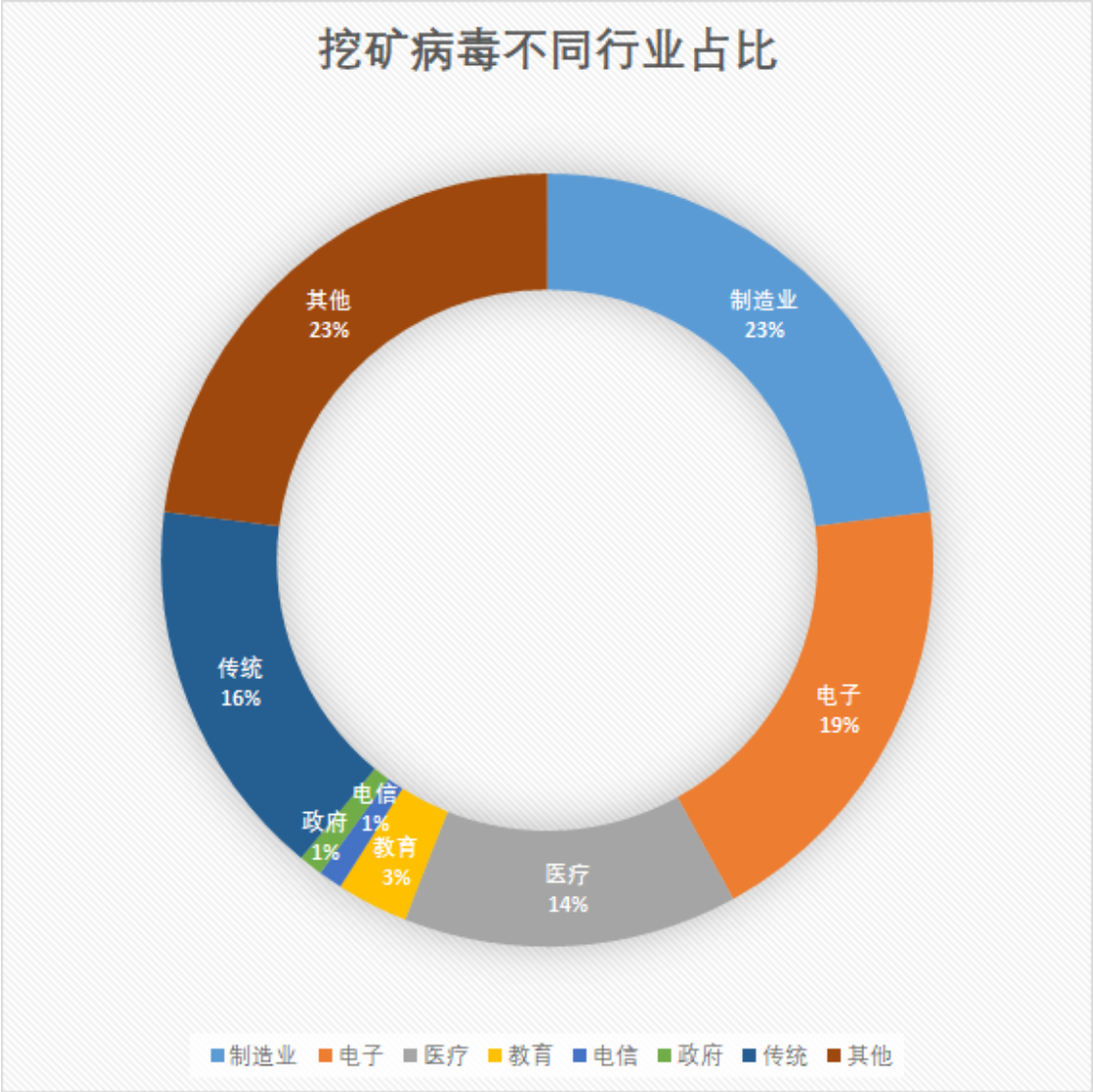
蠕虫、挖矿病毒

2019 年火绒监测到的蠕虫病毒牟利方式多以挖矿为主，蠕虫病毒利用网络服务或者系统漏洞等方式攻入企业服务器，向中毒终端内植入挖矿程序(HackTool/CoinMiner)，使得该服务器成为黑客的“矿机”，从而形成为黑客谋取利益的大型僵尸网络。此类蠕虫病毒通过多种方式在内网横向移动，对于大型局域网来说，如果不使用安全软件进行全网查杀并且对漏洞进行修复，则很容易死灰复燃。

经过火绒梳理，2019 年不同行业中蠕虫病毒占比情况，如下图所示：



2019 年不同行业中挖矿病毒占比情况，如下图所示：



由于蠕虫病毒都在不同程度上使用了漏洞攻击的传播方式，致使这些病毒在互联网中的感染量较多。

如 2018 年末“驱动人生”病毒爆发，并于 2019 年大肆传播，先利用第三方软件升级程序下发蠕虫病毒，再使用多种传播方式在短时间内迅速扩大感染范围，使该病毒成为了 2019 年影响终端数量最多的病毒之一。除此之外，持续更新并利用多种方式传播的 WannaMine、NSABuffMiner、MyKings 僵尸网络相关病毒也依然活跃，在 2019 年病毒感染量中占有一席之地。

火绒现阶段可对“MS08-067、MS17-010、CVE-2019-0708”等高危漏洞进行防御/拦截，除部署安全软件外，及时安装 Windows 更新以修复漏洞，保持良好的计算机使用习惯，也可有效提高终端安全性，防御蠕虫病毒利用漏洞进行的攻击。

感染型病毒

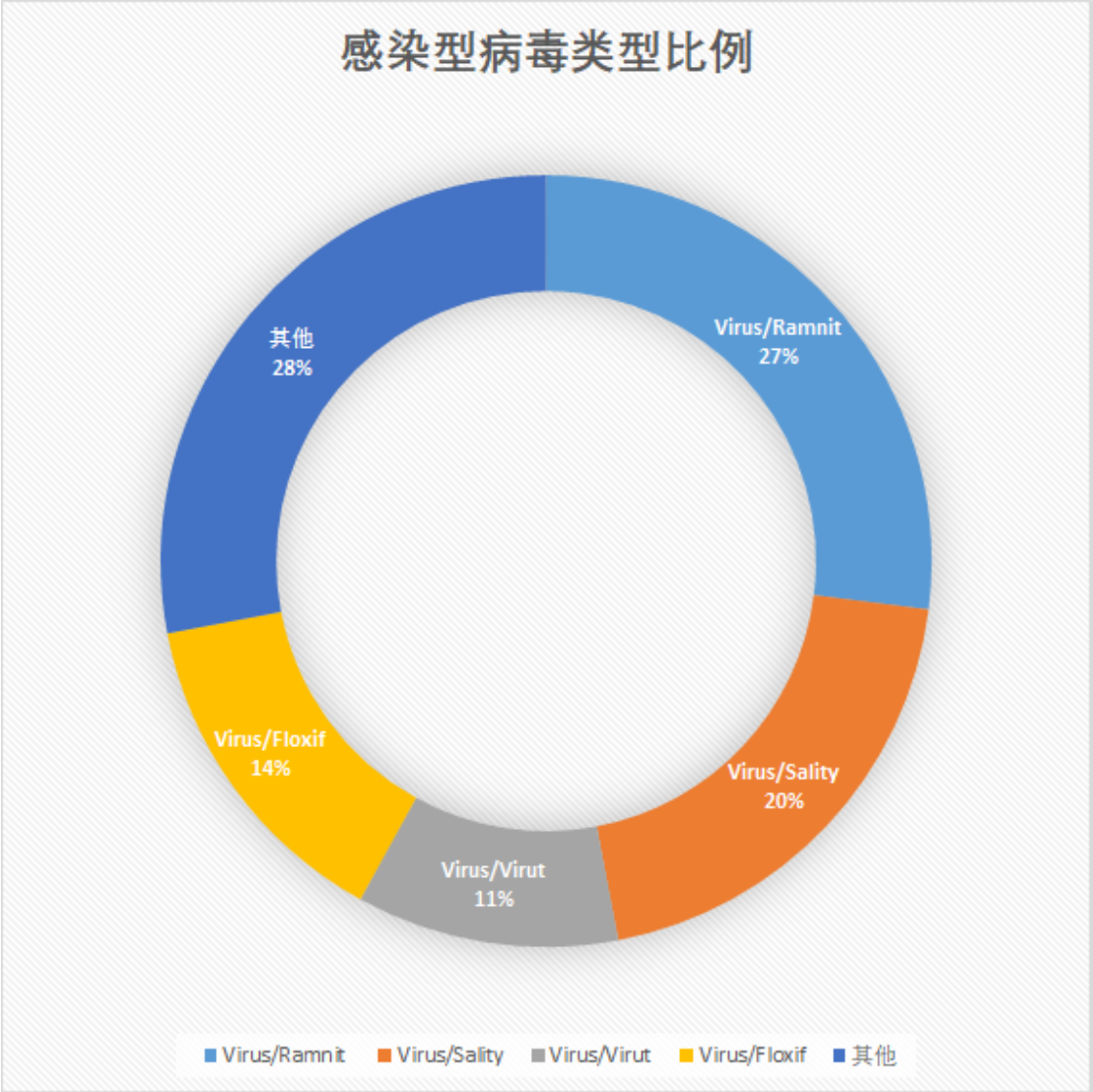
感染型病毒无论在个人用户还是企业用户，都是常见问题。究其原因有以下三点：

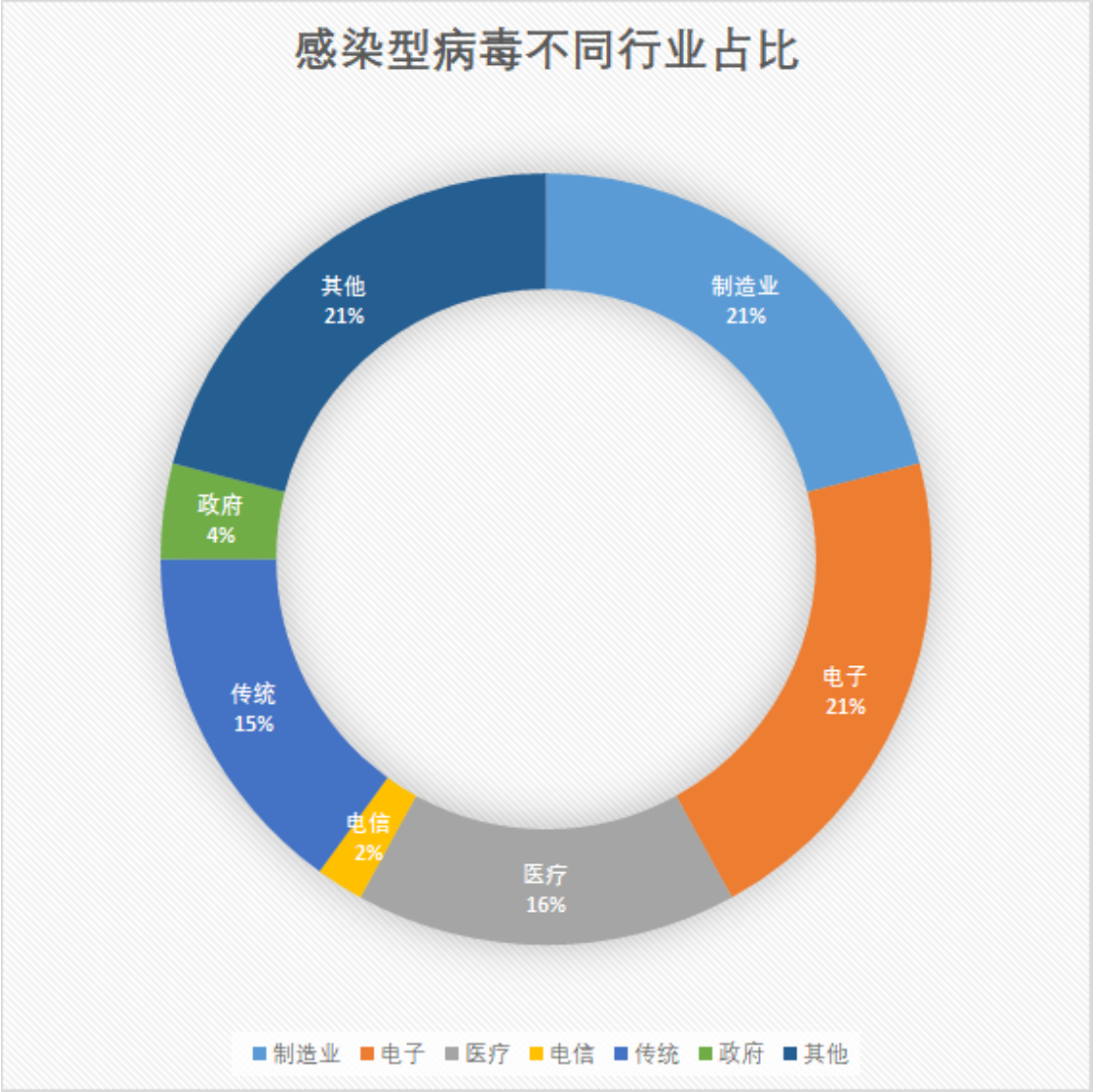
一、感染型病毒会将恶意代码寄生在宿主程序中运行，病毒一旦在用户电脑“扎根”，原本正常的程序可能就会被病毒“寄生”，导致安全软件大量报毒，个人用户往往会误认为安全软件误报了正常程序，从而信任病毒程序，不去处理（相关报告参见附录报告列表 [5]）。

二、根据火绒 2019 年的安全警报可以看到仅“Ramnit”就出现多次。很多企业对安全问题没有足够的重视，对外提供的服务页面、程序就携带感染型病毒。软件发布后包含感染型病毒相关报告，可于附录[6]内查看。

三、对于企业用户，很多新部署火绒终端企业，这些企业之前曾经使用或者正在使用其他安全软件，但是内网依然存在病毒和安全软件共存的现象。主要原因为每个被染毒文件的均不相同，如果没有有效的检测和清除手段，就会出现清除后再次被残留的病毒重新感染。

在 2019 年对企业的技术支持中，我们对遇到的感染型病毒类型和不同行业比例进行了统计，如下图：


感染型病毒类型比例
Virus/Ramnit
27%
Virus/Sality
20%
Virus/Virut
11%
Virus/Floxif
14%
其他
28%
Virus/Ramnit
Virus/Sality
Virus/Virut
Virus/Floxif
其他



以上感染型病毒，火绒个人产品和企业产品均可清除处理（即将被感染文件内的病毒代码清除），清除后不会影响该程序使用。感染型病毒的识别与处理方法，可参考附录[7]内文档。

安全建议

1. 企业内部署火绒企业版终端，并通过火绒中心进行统一配置、管理，定期进行漏洞修复与查杀业务。

2. 定期通过检查火绒、系统和其他安全服务日志，排查企业内可能存在的安全问题。

3. 重要服务器需设置符合复杂性要求的登录口令，多台服务器使用不同的密码管理。关闭或限制不常用高危端口(139、445、3389 等)或相关服务(SMB、RDP 等)，防止配置或使用不当带来的安全风险。

4. 火绒中心防护策略中开启设备控制，注册内网常用的便携设备，对可疑邮件、移动设备，确认火绒检测安全后再打开，减少病毒的传播途径。

5. 个人用户日常使用电脑时，避免非官方渠道下载安装软件，遇到病毒问题及时处理，如有异常日志可联系火绒官方反馈问题。

附录

[1]流量劫持类病毒相关报告列表

《你还在用"加了料"的系统还原工具么？》

https://www.huorong.cn/safe/1565173988349.html

《灰色产业链成病毒传播最大渠道 流量生意或迎来最后的疯狂》

http://www.huorong.cn/info/1563363128323.html

《病毒利用安全产品模块 劫持流量、攻击其他安全软件》

https://www.huorong.cn/safe/1562219029245.html

[2]流氓软件相关报告列表

《“酷我音乐”借“大数据”名义 恐已窥探并收集用户隐私长达数年》

https://www.huorong.cn/info/1577800083411.html

《点击器木马“舟大师”暗刷流量 利用“肉鸡”操纵搜索结果》

https://www.huorong.cn/info/1577721348410.html

《小心这类“李鬼”网站 靠搜索引擎“助力”流氓下载器推广》

https://www.huorong.cn/info/1577158839403.html

《驱动精灵恶意投放后门程序 云控劫持流量、诱导推广》

https://www.huorong.cn/info/1576579765398.html

《金山毒霸"不请自来" 背后竟有黑产推波助澜》

https://www.huorong.cn/info/1552569361195.html

《“WIFI 共享大师”劫持首页推广告 受影响用户高达 20 万》

https://www.huorong.cn/safe/1562218994233.html

[3]第三方软件升级漏洞相关报告列表

《腾讯 QQ 升级程序存在漏洞 被利用植入后门病毒》

https://www.huorong.cn/info/1566134103356.html

《升级漏洞被攻击者“青睐” 阿里旺旺被利用进行病毒投放》

https://www.huorong.cn/info/1568912411370.html

[4]2019 勒索事件回顾

《2019 勒索事件回顾：RDP 弱口令渗透愈演愈烈》

https://www.huorong.cn/info/1578992659420.html

[5]感染型病毒识别、处理方法

《火绒小课堂：“正常文件”被频繁报毒？当心是感染型病毒在作祟》

https://www.huorong.cn/info/1568173581368.html

[6]软件携带感染型病毒报告列表

《VRVNAC 软件携带恶意程序 公安等行业用户可能受影响》

https://www.huorong.cn/safe/1562218994232.html

《火绒安全警报：感染型病毒通过淘宝店传播 窃取用户上网信息》

https://www.huorong.cn/safe/1562218651227.html

《火绒安全警报：“UPUPOO”网站监管力度不严 致带毒壁纸威胁用户》

https://www.huorong.cn/safe/1562813225319.html

[7]火绒使用中常见问题处理

《火绒使用中常见问题处理》

http://down4.huorong.cn/doc/enterprise/faq.pdf