火绒安全
HUORONG SECURITY

2020 火绒终端安全回顾：

流氓病毒化 病毒逐利化

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

目录

前言

2020 年，疫情冲击了各行各业，线上工作需求激增，远程上课、居家办公等一度成为主流，同时也让终端安全防护面临更多的挑战与考验。

在此，火绒根据“在线支持与响应平台”、“火绒威胁情报系统”捕获到的威胁数据，制作并发布本篇《火绒关于 2020 年度终端安全研究报告》，总结本年度互联网终端安全状况，分析全年威胁趋势，为用户提供可行的防护建议。

一、病毒攻势不减　企业个人受威胁类型不同

对于个人用户来说，以 Rootkit 病毒为主。根据平台数据显示，个人用户遭遇到的 Rootkit 病毒占所有病毒数的 58%，恶意行为多以锁定浏览器首页为主，其较为出名的家族 MLXG、SysRoll 等更是在全年不间断更新与安全厂商对抗的技术。

对于企业用户而言，蠕虫挖矿类问题和勒索病毒为最主要的安全问题。两者在所有病毒问题中占比均在 1/4 左右。无论是蠕虫挖矿还是勒索病毒，都在一直持续传播或更新技术模块，并会利用内网渗透的攻击模式，尤其给企业带来巨大的安全威胁。

二、漏洞攻击持续覆盖全网 SMBGhost 成在野攻击新兴漏洞

无论个人版用户还是企业版用户，漏洞威胁一直都是主要的安全议题之一。2020 年我们对漏洞修复、防御方面也在持续跟进，帮助用户预防、抵御安全风险。

对于 2020 年爆出的漏洞来说，在野攻击最为活跃的漏洞为 CVE-2020-0796，由于该漏洞极易被黑客利用，所以在爆出后不久就被黑客加入到了攻击模块中，给互联网安

全造成了一定的影响。

三、广告软件无底线推广　近 98%通过下载器传播

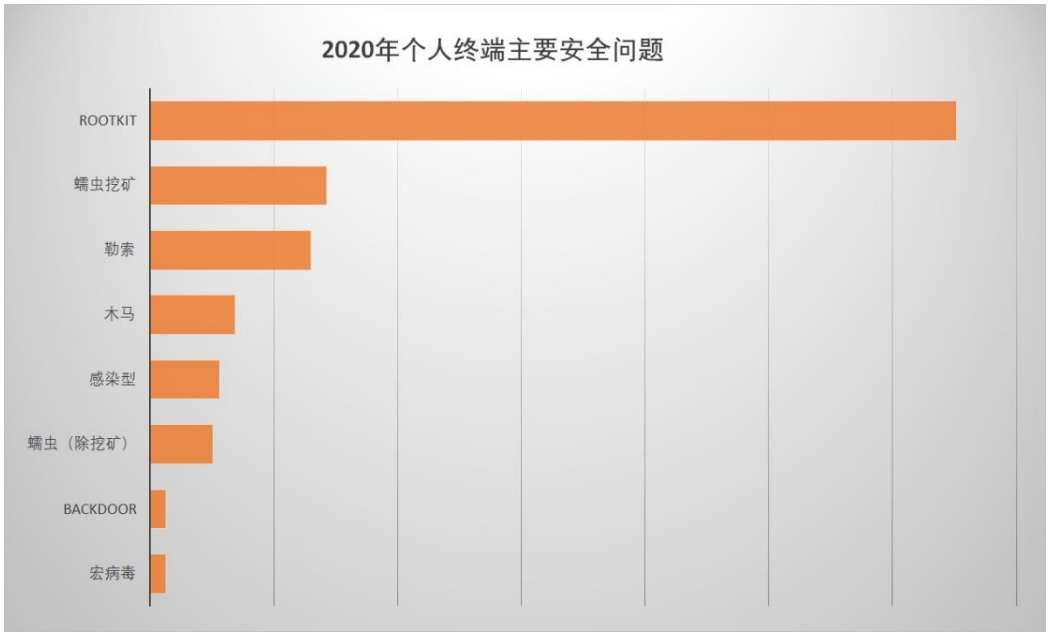
2020 年整年，广告软件问题尤为凸显。从平台数据来看，广告软件绝大部分通过捆绑推广的方式传播，其中，97.88%的广告软件来自下载站下载器推广，仅有 0.21%是用户主动下载安装。此外，2020 年有超过 1/4 的用户电脑遭受过广告软件的侵扰。

广告软件除了疯狂弹窗外，还会静默推广其它软件、替换浏览器中的各类设置、暗刷指定网站的关键字搜索排名、劫持流量，甚至收集用户个人隐私数据、云控“复活”等。基于广告软件无底线传播侵扰用户，火绒在 2020 年也将对其查杀策略调整为彻底查杀。

病毒威胁

个人终端病毒威胁

根据火绒平台数据统计，2020 年个人用户遇到的主要病毒问题是 Rootkit（内核后门病毒）。Rootkit 病毒通常通过灰色软件（激活工具、私服登录器、外挂程序等）进行传播，其恶意行为主要是锁定用户首页。由于部分个人用户对灰色软件存在“刚需”，导致给此类病毒提供了传播渠道。2020 年个人终端主要的安全问题统计情况，如下图所示：

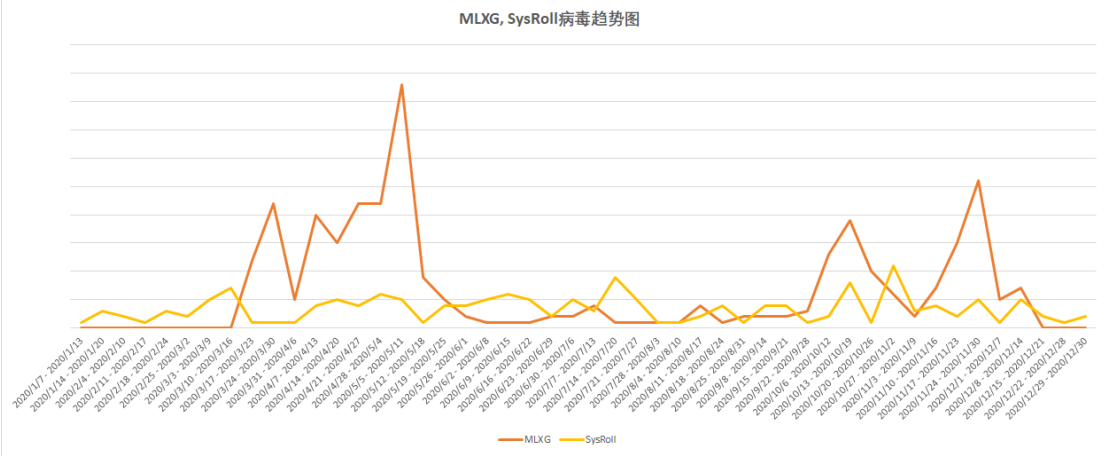


个人终端主要安全问题

Rootkit

Rootkit(内核后门病毒)可以对操作系统内核进行劫持，通过隐藏病毒进程、注册表、文件相关操作等方式与安全软件进行对抗。常见的 Rootkit 会锁定用户首页、劫持流量或者下发其他恶意模块。2020 年 Rootkit 相关报告，见附录报告列表。

2020 年较为活跃的 Rootkit 家族有两个，MLXG 和 SysRoll。根据火绒"在线支持和响应平台"数据统计，在 2020 年 MLXG 和 SysRoll 病毒问题趋势，如下图所示：



2020 年 MLXG, SysRoll 活跃趋势图

MLXG 病毒主要存在于暴风激活、KMS、小马激活等激活工具中，当用户使用上述激活工具后，浏览器首页会被强制锁定为带推广号的网址导航页，并使用内核级对抗手段使安全软件无法正常运行。2020 年出现的 MLXG 病毒，可能是激活工具的缘故，影响的范围较广，每次更新后相关的问题数会明显上升，并且在火绒更新专杀工具后迅速下降。

SysRoll 病毒主要通过传奇私服登录器，传奇私服辅助等进行传播，本身较为小众，影响的范围较小，但也一直活跃和更新。感染 SysRoll 病毒的用户浏览器首页会被强制锁定到传奇私服的页面。

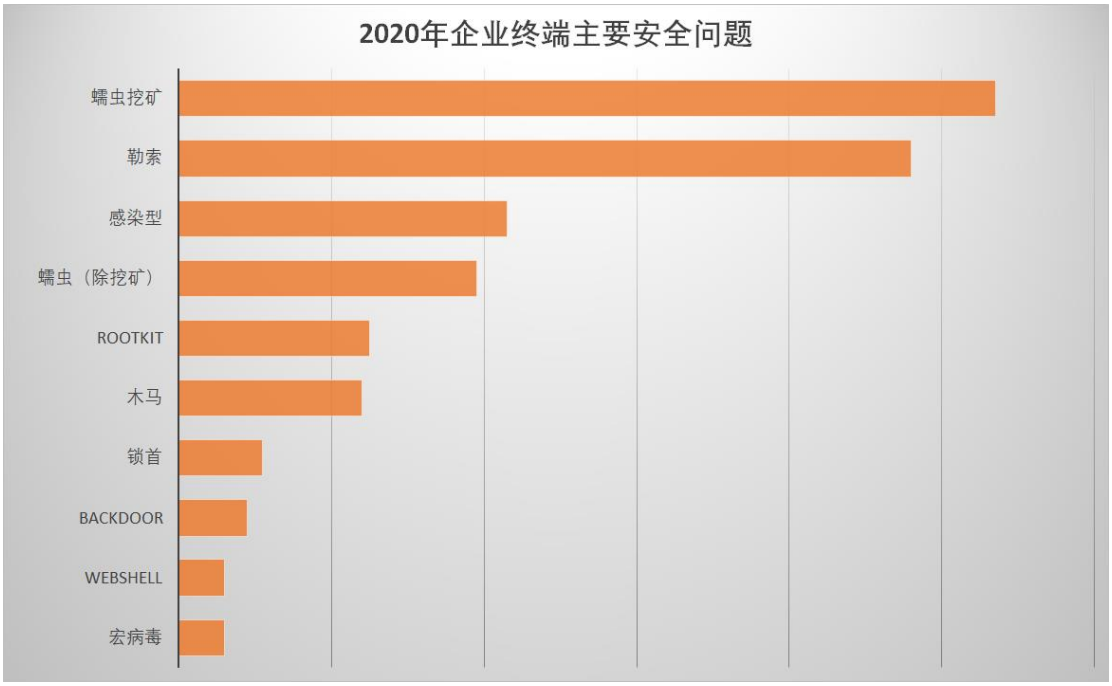
激活工具、私服登录器和外挂辅助等灰色软件是病毒传播的一个重要途径。这些灰色软件会诱导用户在安装时先退出或卸载安全软件，从而躲避杀软查杀。当这些内核后门病毒加载执行后，病毒模块便会受到病毒驱动的保护，普通扫描就无法查杀病毒文件。所以当用户遇到顽固的锁首病毒时，可以尝试使用火绒提供的专杀工具配合全盘查杀清除病毒。

企业终端病毒威胁

对于企业用户来说，2020 年所遇到的安全问题主要集中在蠕虫挖矿问题和勒索病毒问题。此类病毒问题常见的传播手段主要有：系统漏洞、弱口令暴破、共享目录传播等。由于部分企业业务需要员工远程办公，通常将一些运行在本地服务器中的业务发布到公网中。如果这类服务器存在上述安全风险就有可能被攻陷，从而沦为攻击内网的跳

板。

通过平台数据统计，我们发现 2020 年企业遇到的安全问题中，因为此类问题而导致内网沦陷的情况屡见不鲜。2020 年相关报告，见附录报告列表。2020 年企业终端主要安全问题，如下图所示：

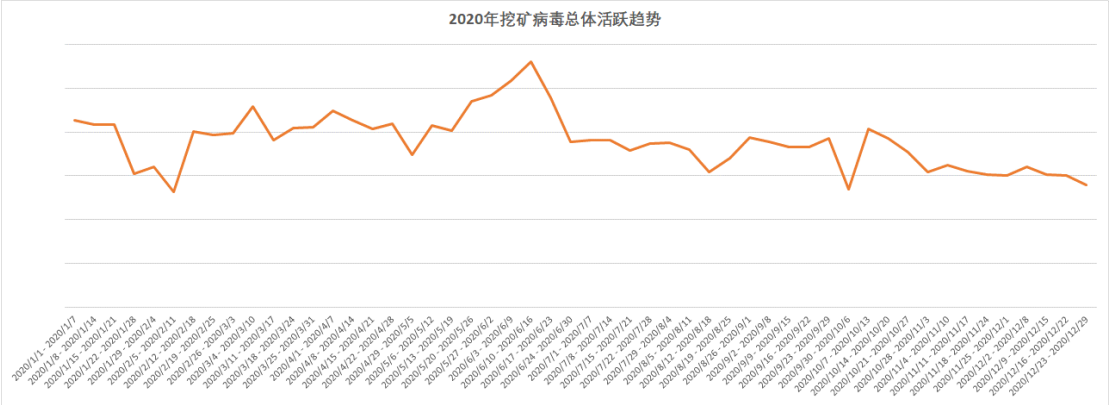


2020 年企业终端主要安全问题

蠕虫挖矿

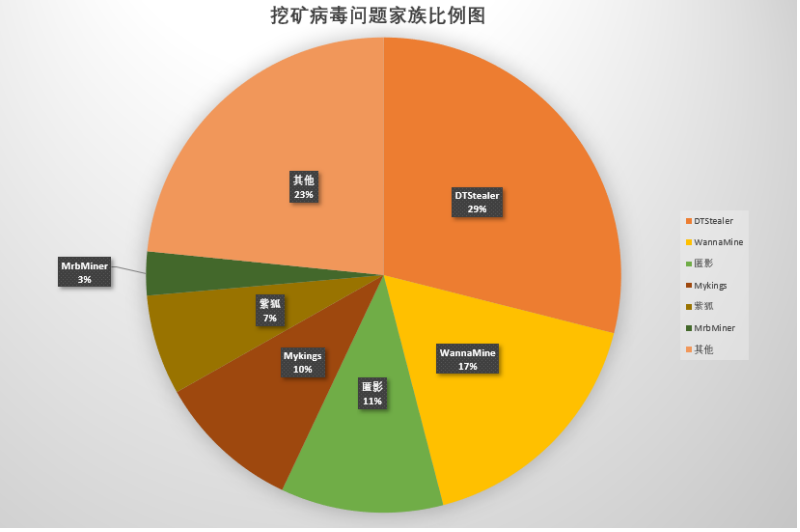
挖矿病毒通过植入挖矿模块到受害主机，占用计算机的计算资源和消耗电力挖取数字货币，从而使机器卡顿甚至卡死，严重影响用户的正常使用。

2020 年多个挖矿病毒家族仍然活跃，传播方式多样且不断进行更新，但整体呈波动下降趋势。2020 年蠕虫挖矿类病毒相关报告，见附录报告列表。2020 年挖矿病毒的总体活跃趋势，如下图所示：



2020 年挖矿病毒活跃趋势

根据火绒"在线支持和响应平台"统计的，2020 年火绒处理的所有挖矿病毒问题中，不同病毒家族所占比例如下图所示：



2020 年挖矿病毒问题家族比例图

在比例图上，主要的挖矿病毒家族都使用“永恒之蓝”漏洞在内网传播。同时一些病毒还可以进行 RDP 爆破、SMB 爆破、数据库爆破等弱口令爆破攻击，感染更多内网中的机器进行挖矿。

在 2020 年火绒跟进响应的挖矿病毒中，DTStealer（又名“驱动人生”或者“永恒

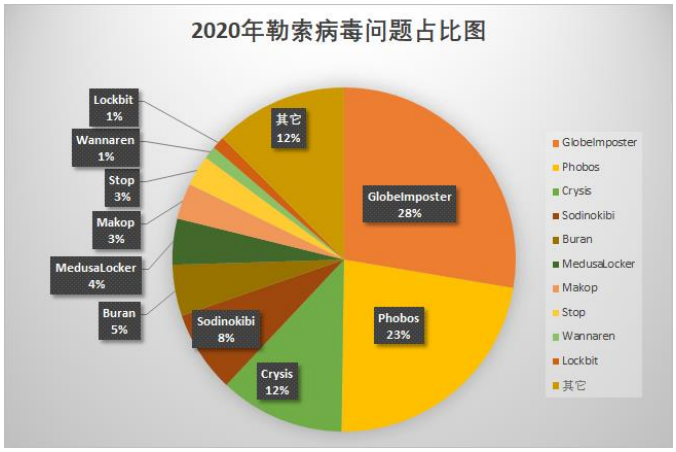
之蓝下载器”）出现的频率最高。相较于其他几个病毒，DTStealer 传播手段更为丰富（集合了”永恒之蓝“漏洞攻击、登录凭证抓取、爆破攻击，感染网络硬盘和移动设备等多种方式），并且紧随安全威胁动态，不断更新组件。比如 SMBGhost 漏洞爆出后不久，DTStealer 便将其加入到横向传播的相关模块中。

火绒不仅可以对挖矿病毒和挖矿组件进行查杀，还可以有效的阻断挖矿病毒在内网中的传播途径。对于永恒之蓝，SMBGhost 等高危漏洞，火绒的网络入侵拦截和对外攻击检测功能可以有效的防御攻击和阻止对外攻击。同时远程登录防护功能可以阻断病毒的 RDP、SMB 等爆破连接，【横向渗透防护】功能也可以有效的拦截病毒的横向传播行为，阻止挖矿病毒的进一步传播。关于【横向渗透防护】功能相关报告，见附录报告列表。

勒索病毒

随着 “勒索即服务”（Ransomware-as-a-Service，简称 RaaS）的勒索病毒运作模式逐渐增多，黑客通过这种运作模式降低了勒索病毒开发和传播门槛，从而扩大了勒索病毒在互联网中的影响范围。在 2020 年火绒跟进响应的主要勒索病毒现场中，排名前五的勒索病毒均使用 RaaS 模式进行运作。

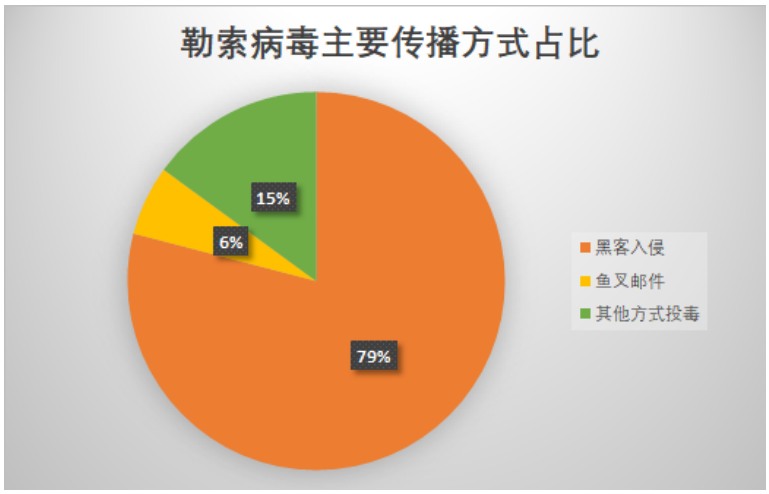
2020 年对互联网影响最大的勒索病毒当属 GlobeImposter、Phobos 和 Crysis，上述三个病毒家族就占据了勒索病毒问题中的绝大多数。2020 年勒索病毒相关报告，见附录报告列表。全年勒索病毒问题占比情况，如下图所示：



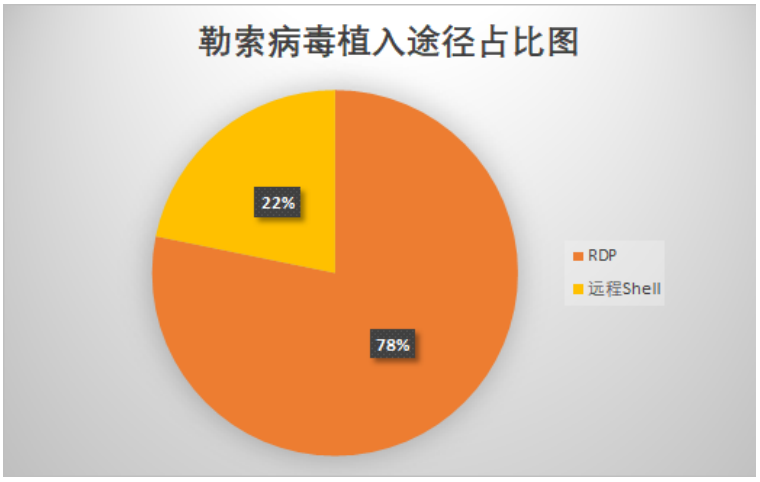
勒索病毒问题占比图

2020 年所遇到的勒索病毒问题中，企业问题高居不下，且企业终端被黑客入侵植入勒索病毒的情况屡见不鲜。

经过火绒分析统计，有高达 79%的勒索病毒攻击事件是由黑客入侵引发。在被黑客入侵的勒索病毒事件中，又有 78%的现场为黑客通过 RDP（Remote Desktop Protocol，即远程桌面协议）远程登录的方式植入、执行勒索病毒。为了躲避安全软件查杀，在黑客远程登录到用户终端后，首先会尝试使用内核级工具、或直接通过安全软件的功能入口结束安全软件进程，再投放勒索病毒对终端数据进行加密，从而提高勒索加密等恶意行为的完成度。相关病毒事件数据，如下图所示：



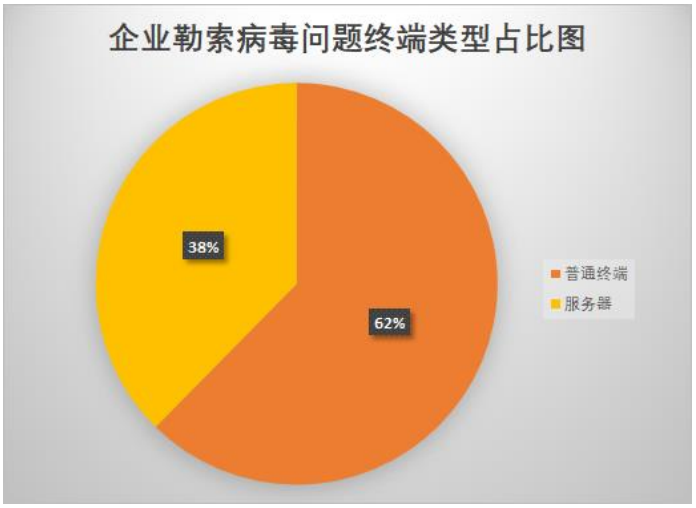
勒索病毒主要传播方式



勒索病毒植入途径占比图

特别需要关注，一些企业内部服务器通常会对外网开放服务端口，进而使此类服务器极易成为黑客进入企业内网的跳板。通过数据统计，我们发现有 38%的勒索病毒问题与企业所使用的服务器相关，甚至个别企业对外网开放的服务器中存在较为严重安全问题，如：弱口令、高危系统漏洞等。

此外，由于企业内部所使用的第三方软件在连接数据库和远程终端时，通常会使用软件提供的默认密码，致使企业使用的财税软件、OA 系统、ERP 管理系统极易成为黑客入侵的突破口。相关数据，如下图所示：



企业勒索病毒问题终端类型占比图

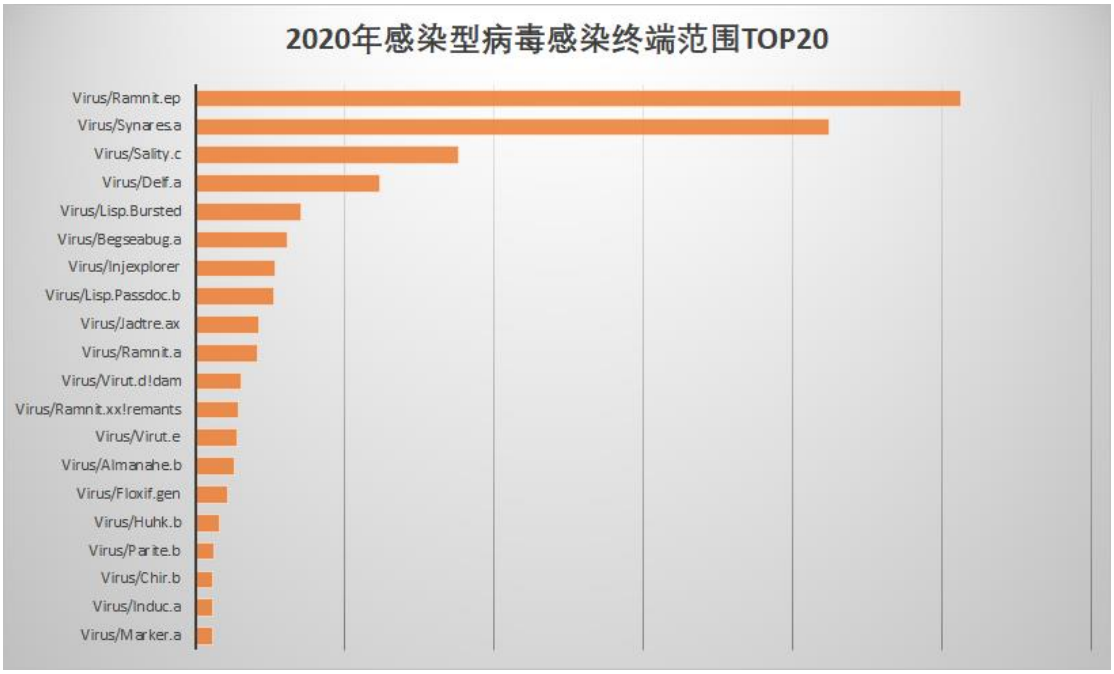
近年来，黑客针对企业用户的勒索病毒攻击事件逐渐增多，数据安全对于企业用户来说愈发重要。如 2020 年 12 月，富士康位于墨西哥工厂的服务器也曾被黑客入侵，数量众多的服务器数据被加密，并被索要上亿人民币赎金。

除勒索外，个别黑客还会在勒索加密数据文件前窃取用户数据，对于不愿交出赎金的用户，黑客会通过“暗网”等渠道泄露用户的关键数据，使中毒用户遭受到严重的数据财产损失。

针对通过 RDP 远程登录执行勒索病毒的攻击现场，火绒企业版中的【终端动态认证】功能，可以帮助用户抵御来自黑客的 RDP 远程登录，从而有效降低黑客勒索加密用户数据的概率。关于【终端动态认证】功能相关报告，见附录报告列表。

感染型病毒

感染型病毒以寄生的方式将恶意代码附着于正常文件中，并通过被感染的文件进行传播。2020 年感染型病毒感染终端范围 Top20，如下图所示：



2020 年感染型病毒感染终端范围 TOP20

感染型病毒不仅可以感染可执行文件，还可以感染文档、带有脚本的工程文件（如 Maya, AutoCAD）、图片、网页文件等。由于被感染的文档只有在执行后才会释放出原始的文档，导致用户为了使用文档而不得不执行病毒，从而使病毒进一步传播，感染更多终端。

对于感染型病毒，火绒的处理策略是清除被感染文件中的病毒代码，同时我们也在不断更新以支持更多的感染型病毒的清除。2020 年火绒新增了对 “Spreadoc”（感染文档）、“普天同庆”（感染 Maya 工程文件）等多种感染型病毒的清除方案。2020 年感染型病毒相关报告，见附录报告列表。

由于企业中大量使用局域网共享和 U 盘进行数据交换，因此当感染型病毒不能及时完整的清除，那么整个内网环境就有可能被反复感染，频繁报毒。感染型病毒的相关

处理方法见附录。

企业安全报告

2020 年度，火绒在为企业提供在线支持与应急响应服务过程时，会对用户常遇到的安全问题，和用户常忽视的安全风险进行归纳与总结，并在火绒对外平台以报告的形式向用户及时预警，帮助企业发现企业网络中可能存在的安全薄弱点，进行针对性的安全加固和防护。

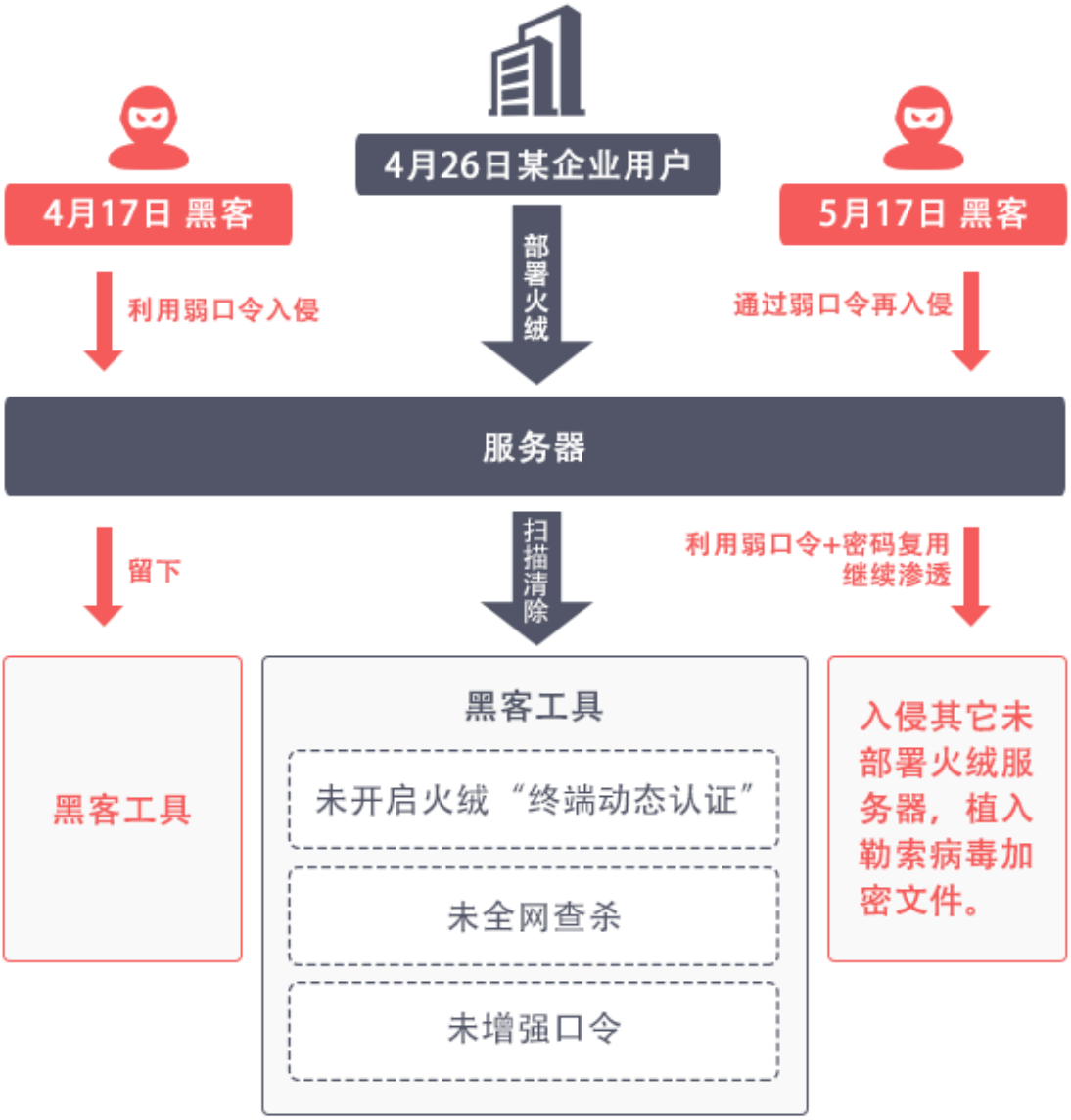
此部分为火绒对本年度“企业安全”相关报告文档进行整理回顾：

“弱口令”问题是本年度火绒对企业提供服务时，最常发现的安全问题之一。

根据火绒火绒工程师全年排查问题发现，造成上述问题原因包括诸如企业未对系统自带的“默认账户”进行管控、系统、业务账号使用的密码强度不足，黑客通过暴破、社工等方式导致企业泄露账号、密码，对企业造成严重安全风险。

2020 年火绒涉及“弱口令”报告如下：

- 《默认账户居然是黑客入侵高频通道 火绒防护措施在这里》
- 《勒索病毒持续高发 企业用户如何警惕弱口令防护短板》

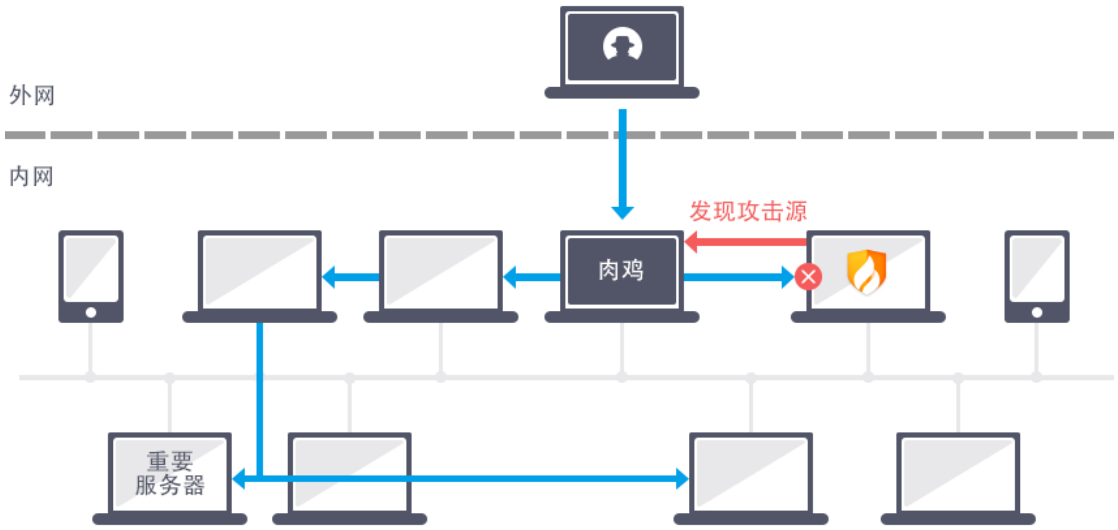


“横向渗透”是企业遭遇的另一大常见安全问题。根据火绒在帮助企业用户处理相关问题时，发现有近半数都涉及到了横向渗透的攻击方式。

黑客一旦从外网进入目标局域网控制某一个终端，就可以利用同一局域网的信任关系，如共享权限、密码、凭据等，入侵其它终端，做更大范围的渗透攻击，由点到面，不断获取并控制高价值的目标终端，最终穿透整个局域网。

2020 年火绒涉及“横向渗透”报告如下：

- 《企业域控服务器遭遇渗透 火绒企业版切断黑客入侵攻击链》



此外，还有一些长期对企业造成困扰的问题，火绒对此类问题进行处理后，也会将问题以报告的方式对其他用户提供支持，期望减少此类安全问题对用户造成的困扰，例如：企业内文件共享可能遇到的安全问题与处理方法、企业内常见挖矿病毒与处理方法、勒索病毒的变化趋势与防护方式等。

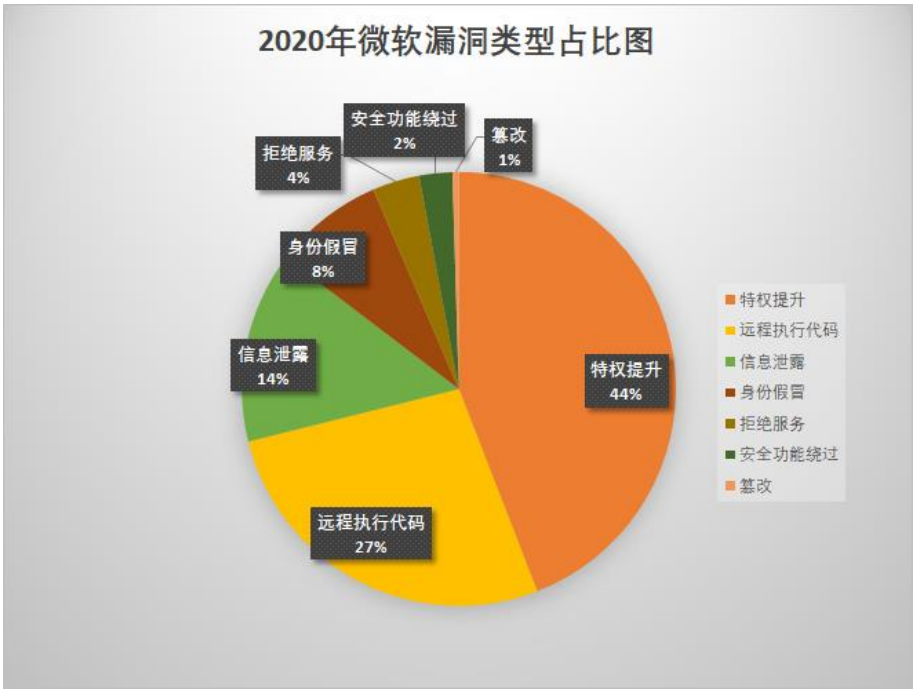
2020 年火绒涉及上述问题报告如下：

- 《企业安全须知：别让共享网络成为病毒传播径道》
- 《根据火绒查杀数据发现 挖矿病毒的套路都在这里》
- 《根据近期勒索病毒变化趋势与响应 揭露企业用户易踩陷阱》

针对企业发起的攻击越来越多，无论是挖矿、勒索还是数据窃取，对企业来说都会造成较大损失，及时以合理、高效的方式加固企业网络安全环境，防御未来可能遭受的攻击。火绒也会持续关注各类安全事件，提供更完善的防护。

漏洞威胁

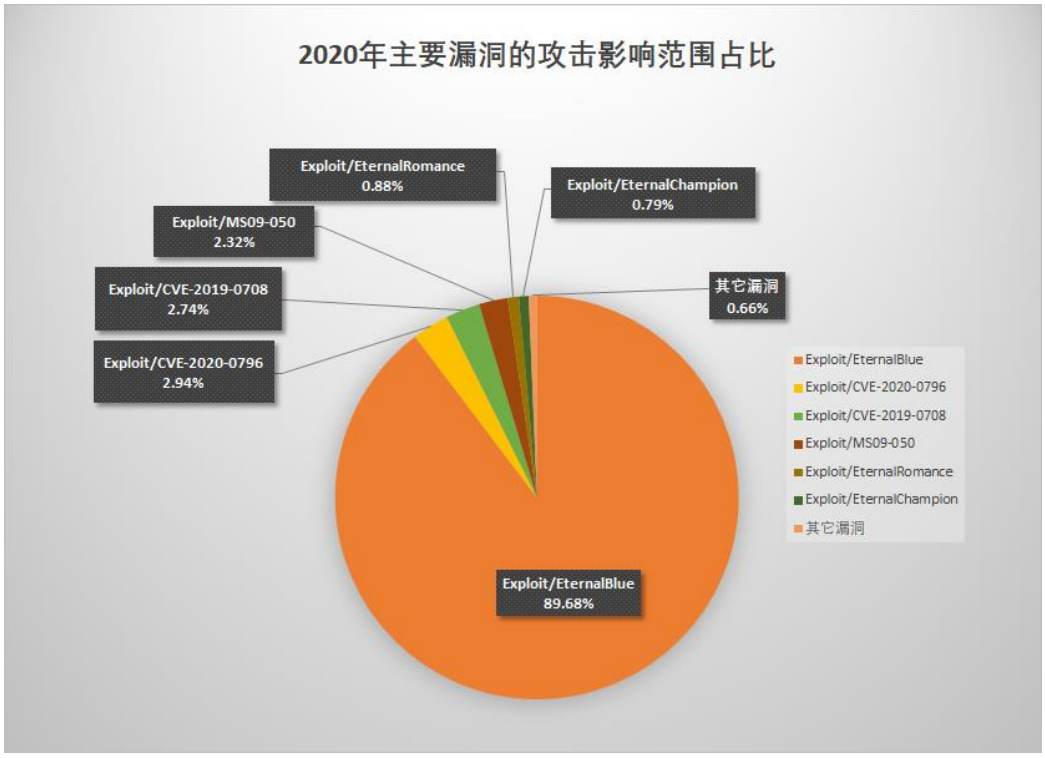
2020 年，微软官方共公布了 1256 个漏洞补丁，其中有 190 个漏洞级别为“Critical”（高危），1057 个为“Important”（重要），火绒都会及时响应预警，并提供修复方式。2020 年微软漏洞类型占比，如下图所示：



2020 年微软漏洞类型占比图

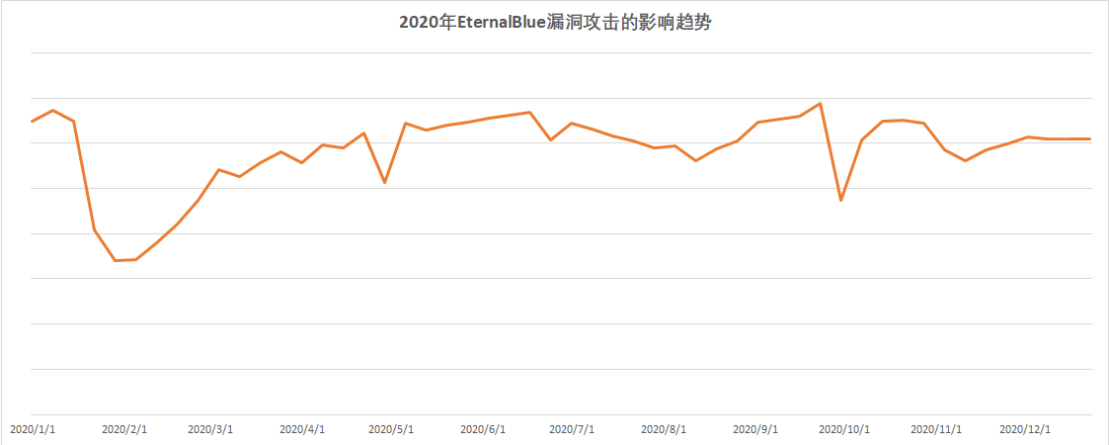
EternalBlue（永恒之蓝）

软件漏洞长期以来都是病毒传播的主要渠道，通过对 2020 年漏洞攻击数据的统计，我们发现远程漏洞攻击中依然以“永恒之蓝”为主，在整体的漏洞攻击事件中占比近 90%。2020 年漏洞攻击总量占比，如下图所示：



2020 年漏洞攻击总量占比

在野进行攻击的漏洞事件中 EternalBlue（永恒之蓝）漏洞占据了绝大多数，使用该漏洞进行传播的病毒主要包括前文中所说的与挖矿相关的病毒家族，如 DTStealer、WannaMine、匿影、紫狐等。2020 年 EternalBlue 漏洞攻击的影响趋势，如下图所示：

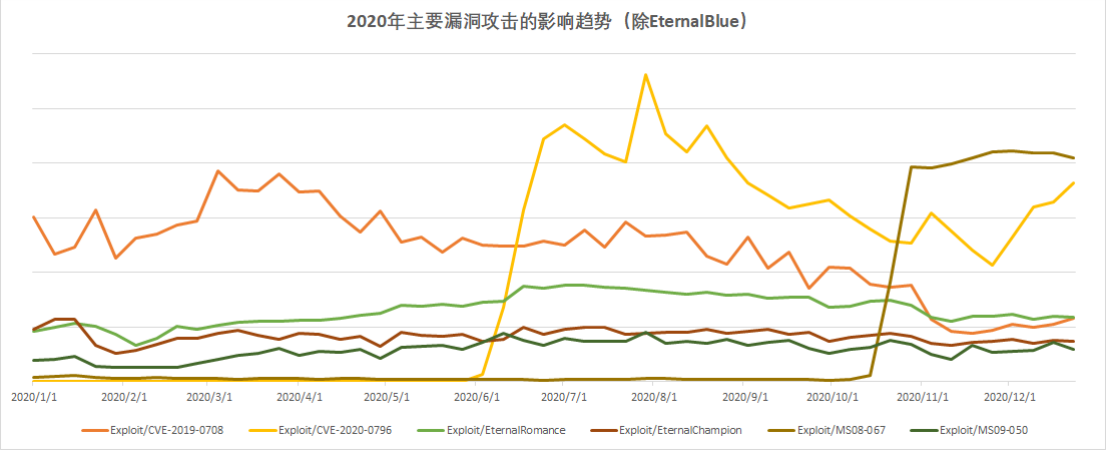


2020 年 EternalBlue 漏洞攻击的影响趋势

CVE-2020-0796（SMBGhost）

2020 年爆出的高危漏洞中，CVE-2020-0796（或 SMBGhost）漏洞对 2020 年互联网安全的整体影响相对较大。该漏洞爆出后，在较短的时间内就被引入到了一些蠕虫病毒（如 DTStealer 等）的横向传播模块中，从而造成了更大范围的安全威胁。

除了新漏洞以外，较为老旧的 MS08-067 漏洞在野攻击情况也依然频繁。除 EternalBlue 外，其他漏洞攻击影响趋势，如下图所示：



2020 年主要漏洞攻击的影响趋势（除 EternalBlue）

其它高危漏洞

在 2020 年爆出的漏洞中，虽然在前文中我们只看到 CVE-2020-0796 漏洞对互联网安全的影响，但是在这一年中还有一些高危漏洞即使现在被黑客使用的频率有限，但也极易被黑客用于进行病毒传播和攻击渗透。此类漏洞列表：

1. Windows TCP/IP 远程执行代码漏洞(CVE-2020-16898)
2. Netlogon 特权提升漏洞(CVE-2020-1472)
3. Windows DNS 服务器远程执行代码漏洞(CVE-2020-1350)
4. Windows NTFS 远程执行代码漏洞(CVE-2020-17096)

5. Windows 网络文件系统远程执行代码漏洞(CVE-2020-17051)

针对漏洞，除了定期使用【漏洞修复】功能进行扫描修复外，还可以通过开启【网络入侵拦截】功能进行防护。我们会不断跟进相关漏洞防御功能，将易被黑客或病毒使用的漏洞加入到相应的漏洞防御规则中，保护用户免受漏洞攻击所产生的安全威胁。

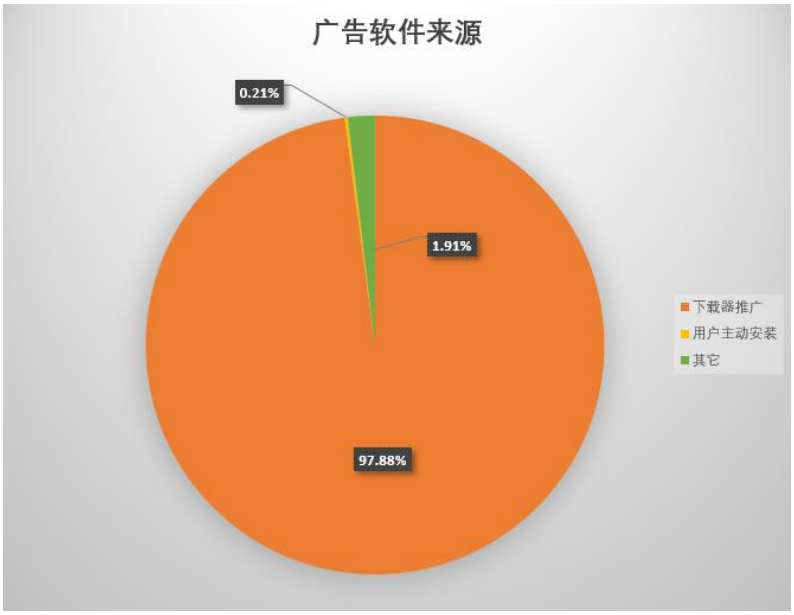
2020 年漏洞相关通告、报告，见附录报告列表。

广告软件

广告软件的来源

广告软件通常没有正规的下载官网，大部分均通过捆绑推广的方式进行传播，且安装较为隐蔽，令用户难以察觉，只有在弹窗时才发现被捆绑安装；即使存在下载官网，整个官网也大都结构简陋，除了提供软件下载链接外不具备其它功能。除此之外，该类软件也会互相静默推广。

面对这些层出不穷，卸载不掉的广告软件，我们统计并归类了 2020 年全年的广告软件类问题发现，用户电脑中的广告软件 97.88%都来自于下载器推广，仅有 0.21%是用户主动下载安装。相关数据如下图所示：



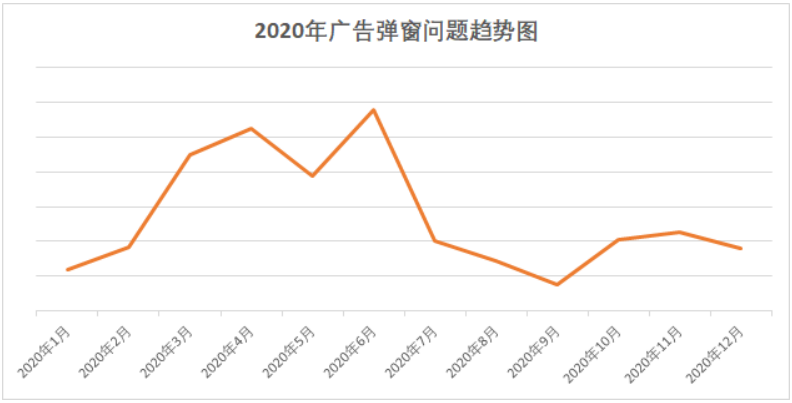
广告软件来源数据统计

由此可见，下载器是广告软件传播的最大渠道，因此我们在【程序执行控制】功能中加入了【下载站下载器】的拦截规则对下载器进行拦截，相关报告见附录报告列表。

广告软件的危害

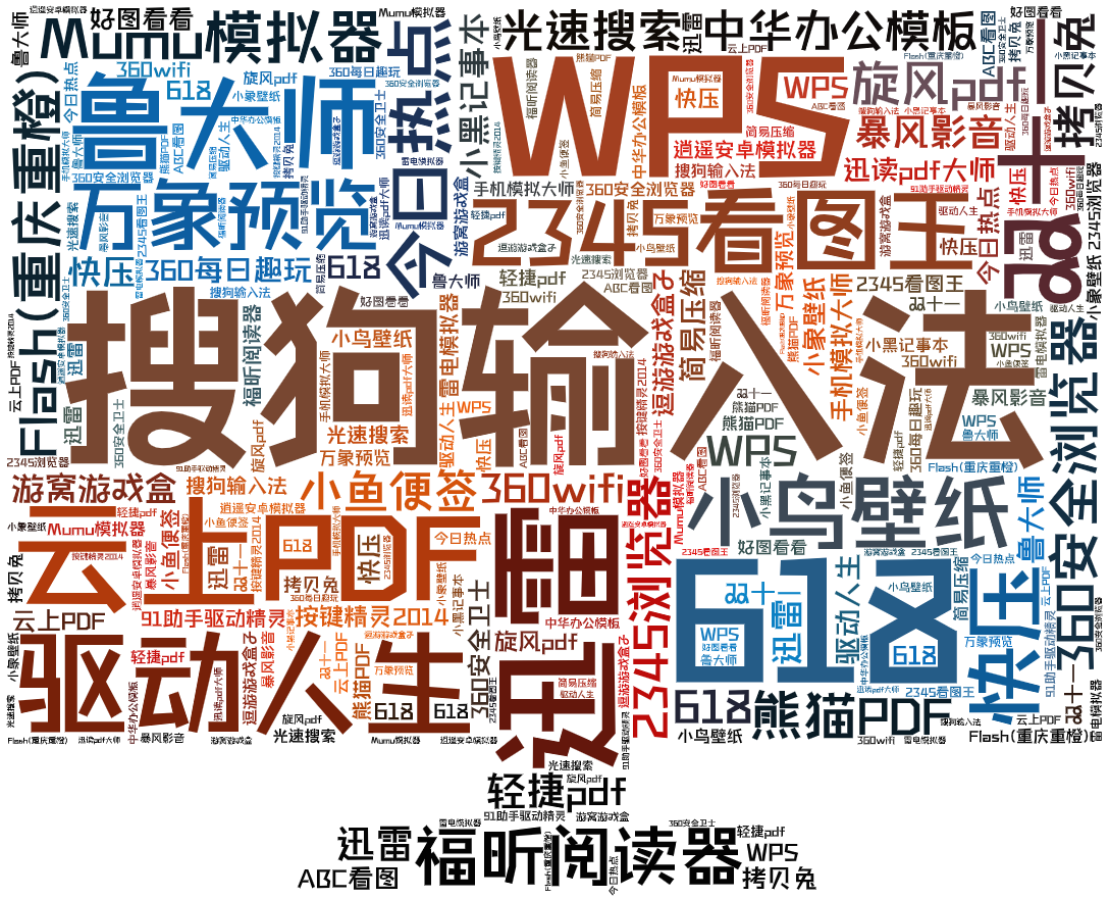
相比于其它恶意病毒攻击事件，广大用户在日常生活中更容易被广告软件所困扰。在 2020 年，火绒针对广告软件进行了持续追踪，该类软件长期霸占用户电脑用以牟取利益。

首先是广告弹窗骚扰。2020 年中，根据火绒“在想支持和响应平台”对广告弹窗相关问题的统计，我们发现自疫情复工开始到“618”电商活动前后，广告弹窗问题逐渐凸显。从去年问题趋势来看，“双十一”和“双十二”前后虽然相对于上半年数据增长不明显，但总量也有所增加。2020 年广告弹窗问题趋势图，如下图所示：



2020 年广告弹窗问题趋势图

通过统计 2020 年全年广告弹窗问题相关的关键词，我们将问题出现频率较高的关键词以词云的形式进行了汇总。广告弹窗问题相关关键词热度，如下图所示：

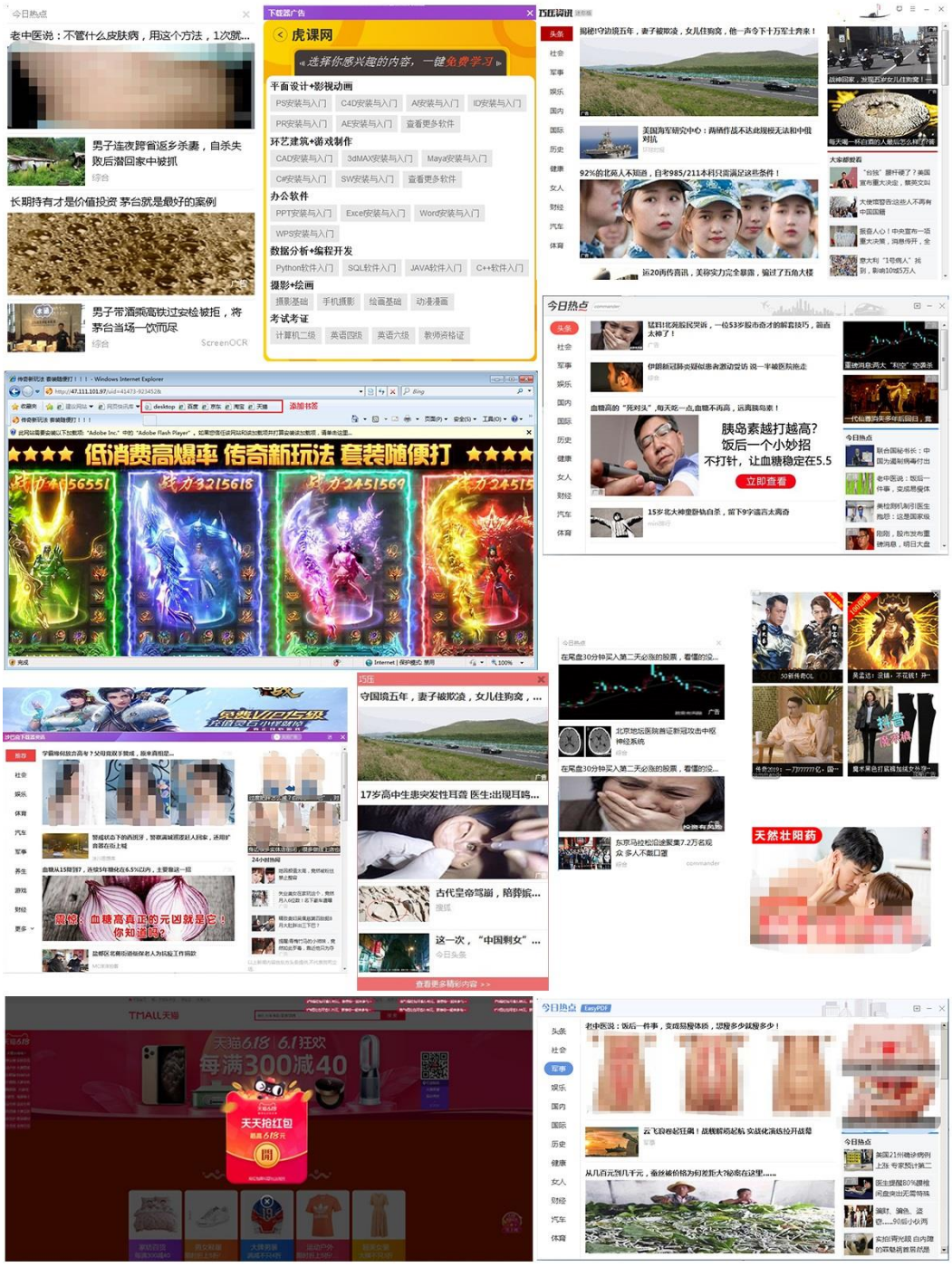


广告弹窗问题相关关键词热度

广告软件除了花样百出的弹窗方式之外，还具有如下恶意行为：静默推广其它软件、替换浏览器中的各类设置，包括首页、书签、收藏夹、新标签页、历史记录等、暗刷指定网站的关键字搜索排名、劫持流量、收集用户个人隐私数据、云控“复活”等。

更令人意想不到的是，一些大型软件厂商凭借用户基数大，粘性高也会做出上述广告软件相关的越权行为，严重降低了用户的软件体验感及信任度。

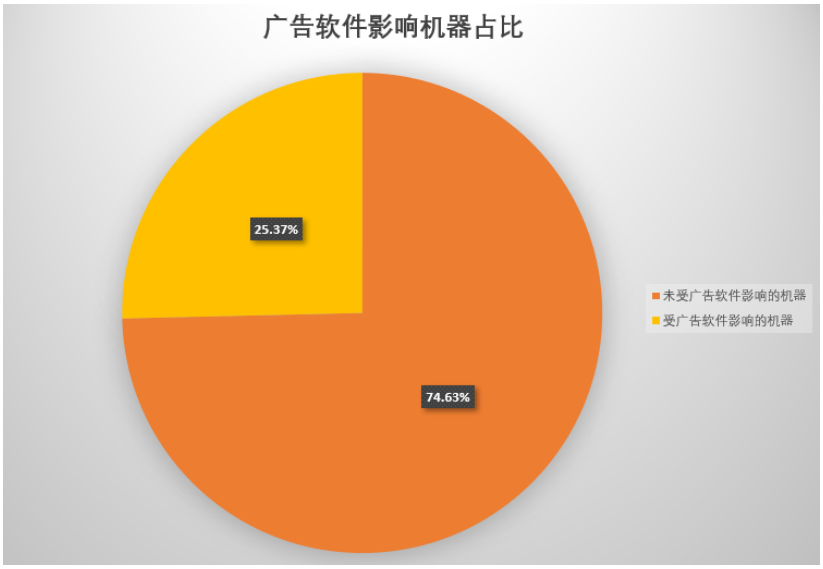
由于用户早已习惯此类软件的使用，即使得知该软件具有广告软件类恶意行为，也只能被动接受，从而导致这些软件厂商在用户电脑上更加肆无忌惮，为所欲为，受害用户苦不堪言。火绒 2020 年相关报告，见附录报告列表。相关弹窗广告，如下图所示：



广告弹窗图

广告软件的受害比

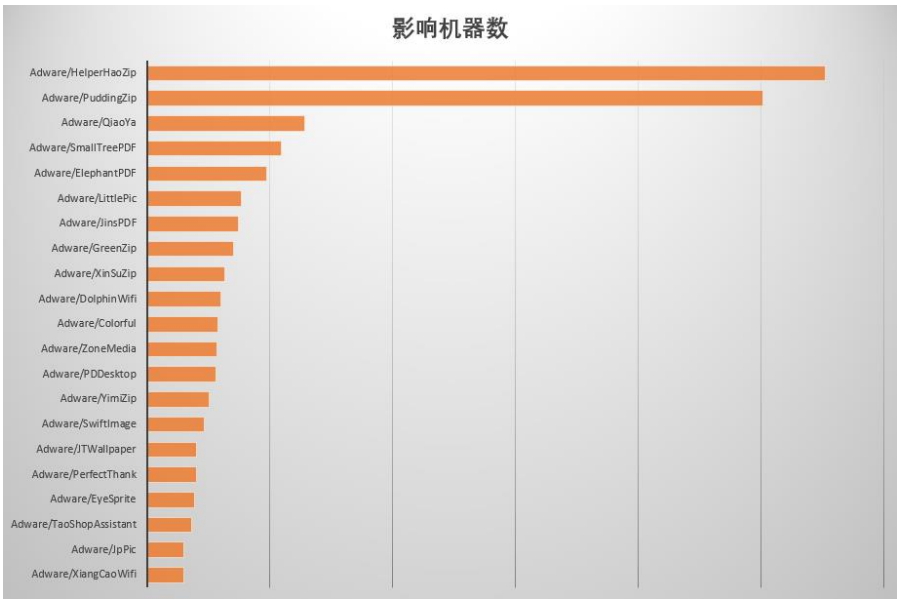
广告软件数量庞大，受害用户数不胜数。我们统计了 2020 年全年相关数据发现，超过四分之一的用户都遭受过广告软件的侵扰。相关数据如下图所示：



广告类病毒机器占比

广告软件家族 TOP20

广告软件家族众多，我们统计了 2020 年全年各个广告软件家族所影响的机器数，并做出 TOP20 排名。值得一提的是，和去年所统计的广告软件家族排行相比“Adware/HelperHaoZip”依旧稳居第一。相关数据如下图所示：



2020 年广告软件家族 TOP20

广告软件查杀策略变化

在如今流量既是利益的环境下，广告软件的弹窗，推广等恶意行为更加疯狂，甚至这些软件逐渐批量化，产业化，规模化。部分还会通过规避城市，躲避安全软件等方式与安全软件进行对抗，长久扎根于用户电脑之中。

针对此类软件的恶意行为，火绒也一直积极开发并完善相关功能来保护用户电脑。如：【文件实时监控】、【软件安装拦截】、【下载器拦截】、【弹窗拦截】等。

但是由于广告软件自身的特殊灰色性质，增加了部分安全厂商对其鉴定的难度。这也导致了此类软件愈发层出不穷，肆无忌惮的把用户电脑当成牟取利益的赚钱工具，逐渐越过安全底线，尽最大可能的榨干用户电脑存在的流量、隐私价值。让用户及部分安全厂商处于对抗的劣势方。仅靠提示拦截已经不足以帮助用户免受广告软件的侵犯，我们决定在严格判断、认定后，将彻底查杀此类软件，不给其更新、“复活”对抗的机会。查杀程度随之升级，由此前的查杀部分广告模块覆盖为整个广告软件，彻底杜绝广告软件的侵扰。

附录

[1]广告软件相关报告列表

《今天你被“PUA”了吗？》

https://www.huorong.cn/info/1590374126479.html

《火绒将彻底查杀广告软件 首批包括 50 余款》

https://www.huorong.cn/info/1605764777553.html

《装机工具老毛桃携带木马病毒 卸载安全软件进行恶意推广》

https://www.huorong.cn/info/1598957552515.html

《从流氓推广到公然投毒 流氓软件完成黑化》

https://www.huorong.cn/info/1595425144501.html

《木马程序借助“游民星空”等下载站再次大肆传播 可云控投放恶意模块》

https://www.huorong.cn/info/1594297526495.html

《搜狗输入法强制推广“618 红包广告” 用户不堪其扰》

https://www.huorong.cn/info/1591365611484.html

《无节制流氓推广 2345 旗下下载站正在传播木马程序》

https://www.huorong.cn/info/1583504456441.html

《流氓软件巧压卸载仍留恶意模块随时“复活” 一招教你彻底清除》

https://www.huorong.cn/info/1582805565440.html

《“去广告”插件云控劫持流量 产品官网假坦然“求同情”》

https://www.huorong.cn/info/1582284212427.html

[2]下载站下载器拦截功能相关报告

《不想再走下载器的套路？ 你要的火绒拦截功能来了》

https://www.huorong.cn/info/1585649020449.html

[3]Rootkit 病毒相关报告列表

《一文揭露各类劫持浏览器主页手段 附火绒修复方式》

https://www.huorong.cn/info/1606367590557.html

《激活工具散播锁首病毒“麻辣香锅“ 诱导用户退出安全软件》

https://www.huorong.cn/info/1589940017463.html

[4]渗透入侵相关报告列表

《默认账户居然是黑客入侵高频通道 火绒防护措施在这里》

https://www.huorong.cn/info/1602750290522.html

《使用远程工具也有风险？火绒新增这两个功能可有效防御》

https://www.huorong.cn/info/1592912077490.html

《勒索病毒持续高发 企业用户如何警惕弱口令防护短板》

https://www.huorong.cn/info/1591171443483.html

《企业域控服务器遭遇渗透 火绒企业版切断黑客入侵攻击链》

https://www.huorong.cn/info/1588155233461.html

[5]蠕虫挖矿类病毒相关报告列表

《根据火绒查杀数据发现 挖矿病毒的套路都在这里》

https://www.huorong.cn/info/1595904134505.html

《蠕虫病毒“柠檬鸭”持续扩散 多种暴破方式攻击用户电脑》

https://www.huorong.cn/info/1586944971456.html

[6]横向渗透防护相关报告列表

《火绒个人版新增“横向渗透防护功能” 开启和使用方式都在这里》

https://www.huorong.cn/info/1609132809562.html

《火绒上线“横向渗透防护”功能 竖立内网安全的护城墙》

https://www.huorong.cn/info/1609136353563.html

《企业安全须知：别让共享网络成为病毒传播径道》

https://www.huorong.cn/info/1600305944518.html

[7]勒索病毒相关报告列表

《我们翻出火绒工程师压箱底的勒索病毒自救秘籍》

https://www.huorong.cn/info/1598868041514.html

《根据近期勒索病毒变化趋势与响应 揭露企业用户易踩陷阱》

https://www.huorong.cn/info/1597729969511.html

《警惕“有偿修改代码”陷阱或为勒索病毒在诱骗》

https://www.huorong.cn/info/1596106334507.html

《从“党妹被勒索”事件看 NAS 系统安全》

https://www.huorong.cn/info/1588243403462.html

《勒索病毒不要赎金或跟风“WannaRen"火绒已解密并阻断传播渠道》

https://www.huorong.cn/info/1587695065459.html

《WannaRen 勒索病毒溯源新进展 或通过下载站大量传播》

https://www.huorong.cn/info/1586357607452.html

《回顾 WannaRen 勒索病毒一生：从传播到解密享年 6 天》

https://www.huorong.cn/info/1586519906455.html

《通达 OA 系统用户遭遇勒索病毒攻击的初步说明》

https://www.huorong.cn/info/1584091538444.html

[8]火绒动态验证功能相关报告列表

《火绒终端动态认证功能上线 为企业防护勒索病毒再筑防线》

https://www.huorong.cn/info/1582697039430.html

《火绒产品公告——企业版推出“终端动态认证”功能 阻止 RDP 弱口令渗透》

https://www.huorong.cn/info/1582608651429.html

《火绒产品公告——企业版新增动态口令功能 二次验证加强中心安全》

https://www.huorong.cn/info/1582541663428.html

《聊一聊让微软谷歌等巨头心心念念的“多因素认证”》

https://www.huorong.cn/info/1585039969447.html

[9]感染型病毒相关报告列表

《白担心了 原来火绒这样清除病毒并不会删除文件》

https://www.huorong.cn/info/1607935403560.html

《老病毒借助文档传播活跃七年 目前仅火绒可彻底清除》

https://www.huorong.cn/info/1593514349494.html

《玛雅软件用户请注意 “普天同庆”病毒将于三日后发作》

https://www.huorong.cn/info/1592918228491.html

[10]高危漏洞通告相关报告列表

《2020-12 微软漏洞通告》

https://www.huorong.cn/info/1607500182558.html

《2020-11 微软漏洞通告》

https://www.huorong.cn/info/1605074960523.html

《微软 TCP/IP 远程执行代码漏洞（CVE-2020-16898）风险通告》

https://www.huorong.cn/info/1602673429521.html

《NetLogon 特权提升漏洞验证代码公开 修复漏洞即可防御》

https://www.huorong.cn/info/1600150176516.html

《SMBGhost 漏洞数月后再被“捧红” 火绒用户无需恐慌》

https://www.huorong.cn/info/1591163339482.html

《微软再曝高危远程代码执行漏洞 临时防护措施戳这里》

https://www.huorong.cn/info/1585039969447.html

《微软发布“蠕虫级别”漏洞补丁 相关修复方法及问题解答在这里》

https://www.huorong.cn/info/1584081901443.html

《Win10 最新“蠕虫级别”高危漏洞说明及临时防御措施》

https://www.huorong.cn/info/1584003786442.html

《微软公布新的欺骗性漏洞 无法被利用直接攻击和传播》

https://www.huorong.cn/info/1579257251422.html