Computer System Networking and Telecommunications, 计算机系统网络和电信 (2)2020,2
ISSN:2661-3719(Print)

Windows 系统中的计算机病毒及防范措施

王　春　郭晓丹
四川大学锦城学院　四川　成都　611731

【摘　要】在信息化的时代，各行各业都需要 Windows 系统。它在方便我们生活的同时，也产生了种类、数量繁多的计算机病毒，他会直接对我们的 Windows 计算机造成危害，进而对我们的隐私、经济、生活造成坏的影响。我们必须正确认识计算机病毒带来的危害，用正确的方法进行防范。

【关键词】Windows；计算机病毒；特点；危害；防范

据百度流量研究院统计，截止 2020 年 3 月 29 日全国操作系统用户中 Windows 系统占比 89.75%，如 1 图所示。

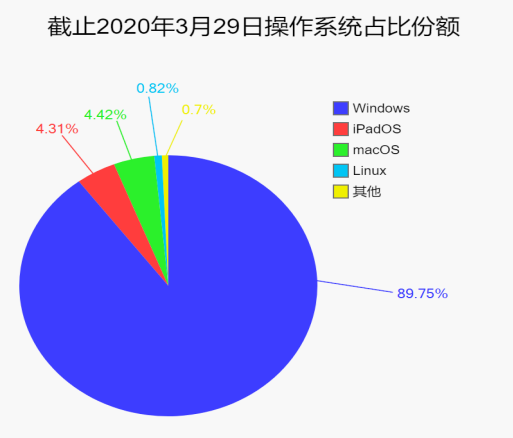

图 1 截止 2020 年 3 月 29 日全国操作系统占比份额

在我们的生活中有着重要作用。然而，由于 Windows 系统用户数量的不断增加，恶意病毒攻击计算机的事件也在逐步增加。且计算机病毒多样化、顽固、难以发现和清除。小到个人信息泄露、电脑崩溃、经济损失，大到企业单位大数目资金亏损。人民权益正在遭受威胁。

1 计算机病毒的含义

计算机病毒（Computer Virus）是指制造者在计算机运行程序中恶意插入的能破坏计算机功能、影响计算机正常使用、能进行自我复制的指令或程序代码。通常不会单独存在，往往是隐藏于其他文件中躲避用户的查杀，我们称这种具有破坏行为的程序为计算机病毒 [1]。

2 Windows 常见病毒的特征

2.1 扩散性

扩散性也叫传染性，是计算机病毒的一大特征，一旦计算机受到感染，病毒就会在计算机中寻找可以充当传播媒介的程序或文件。然后进行自我复制，从当前存储位置扩散到其他未感染的存储位置，尤其是在现在网络发达的条件下其可以通过 Internet 在计算机与计算机之间进行传染，这一途径传播速度最快，感染范围最广，破坏性最强。

2.2 一定的潜伏能力

寄生于其他程序上是计算机病毒的一大特征，这种程序我们称之为宿主。当病毒感染系统内正常的程序后它并不会立刻运行，相反会隐藏自己等待合适的时机对计算机进行攻击。如在一个特定的时间 3 月 2 日才发起攻击。

2.3 破坏性

病毒一旦感染计算机，则系统的稳定性也会受到一定影响。在病毒刚刚激活期间，病毒会进行自我复制，此时会占用系统大部分资源，严重的会使整个系统数据丢失、瘫痪、崩溃。对于企业来讲若遭受这种情况会对企业的经济造成极大的影响。

2.4 隐藏性

计算机病毒往往隐藏在正常的程序中，或直接与系统文件名相似，比如 Windows 系统中 Sys32 文件夹可能会被命名为 Sys22 等相似的文件名；亦或直接伪装成 EXE 可执行程序，一旦用户运行这个可执行程序，就会激活病毒，让人难以察觉。也会隐藏于系统更深层的位置，如注册表等。

2.5 可执行性

计算机病毒可以被触发启动，只需要一个特定的条件。例如执行特定的一个程序、输入一个字母或一个单词等。

3 Windows 计算机病毒的传播途径

3.1 附着在移动设备上以传播感染

移动设备体积小、方便，如：U 盘、移动硬盘、MP3、CD 这些设备。一台 Windows 计算机感染了病毒，又插入了 U 盘，这个病毒便会感染 U 盘，并隐藏于 U 盘中。当另一台电脑使用这个 U 盘后，病毒就会对其攻击。如“文件模仿者病毒”，他一般通过 U 盘等移动设备进行传播，隐藏在 U 盘里等待使用者将 U 盘插入计算机，一旦计算机访问被感染的 U 盘，病毒就会攻击此计算机，隐藏系统文件夹，并生成和系统文件夹同名的文件夹以迷惑用户。一旦用户打开此文件夹，便会出现大量弹窗广告且无法关闭、锁定用户浏览器主页、修改系统 Hosts 文件等。

3.2 通过网络传播

其一，Windows 计算机一旦连接网络，病毒便会趁机通过局域网进行传播，感染局域网中的其他计算机，随后进行破坏。其二，病毒会嵌套在部分网站的文件中，当用户在该网站下载文件时，便会感染自己的计算机。其三，利用 QQ、微信、邮箱等社交软件进行传播，当用户从网上下载不明文件或访问不安全的链接后可能会受到病毒攻击。例如 2006 年在欧洲蔓延的“风暴蠕虫”病毒，它通过虚假的邮件标题诱惑用户点击，用户单击连接后便在后台自动下载病毒。一旦受感染，可在极短时间内感染数千台电脑，最终导致这些电脑瘫痪。再如 2003 年出现的 Sobig 病毒，他通过网络进行传播，他会查找局域网内的其他计算机，破坏其他计算机，在联网状态下还会每隔一定的时间到制定的网址下载病毒，感染邮件，再以邮件为媒介进行传播。

3.3 利用系统漏洞和程序的安全不足传播

Windows 系统和程序因开发量大，所以难以做到完美，不法分子会研究其当中的安全漏洞，利用这个弱点进行攻击、渗透。对我们的计算机造成威胁。如 2017 年的“勒索病毒”，制造者利用 Windows 系统漏洞进行攻击，在极短时间内便在全球扩散，导致数万台电脑的文件数据被加密，向用户索要高额赎金来解锁电脑。再如 2011 年出现的 Duqu 病毒，他利用了 Windows 系统的漏洞对计算机进行攻击，他可以盗取受攻击系统中的所有信息，并且具有隐藏性，这为犯罪分子进行工业间谍活动提供了不小的帮助，甚至勒索受害用户。

4 计算机病毒的分类

4.1 病毒传播的方式

（1）网络病毒：指通过网络传播、具有感染破坏计算机可执行文件能力的病毒。此类病毒传播范围很广，传播速度很快，感染性很强，严重时可导致网络瘫痪。

（2）文件病毒：主要感染计算机中的可执行文件和命令文件，可以修改文件并且感染文件。文件型病毒主要传染 .COM 文件和 .EXE 文件。

（3）引导性病毒：指寄生在磁盘引导区或主引导区的计算机病毒，他会将病毒传染给计算机的软盘和硬盘，并且监视系统运行，等待时机进行破坏。

4.2 病毒的传染方法

（1）驻留型病毒：此类病毒感染计算机后会将自身的一部分内存留在 RAM 中，且处于激活状态，直到关机或重新启动。

（2）非驻留型病毒：此类病毒只会在特定的条件下才被激活，并不会一直处于激活状态，进而感染其他计算机。

4.3 病毒的危害

（1）无危险病毒：此类病毒不会对系统有太大影响，它只会降低用户可用的运行内存、使磁盘繁忙等。

（2）危险病毒：会对系统造成影响，如破坏计算机中的数据，破坏系统组件、恶意删除程序，恶意下载程序等，造成系统崩溃关机的病毒。

（3）伴随型病毒：并不改变文件本身，会根据算法产生文件名相同但扩展名不同的可执行程序。

（4）“蠕虫”型病毒：一种通过网络传播的恶意病毒，一大特点是可以不依赖于宿主程序而独立运行，主动实施攻击，且传播速度是普通病毒的数百倍。

（5）寄生型病毒：他和“蠕虫”型病毒最大的区别在于寄生型病毒需要寄生在宿主上，一旦宿主被运行，病毒也随之被激活。

5 计算机病毒对 Windows 系统的危害

大部分病毒在进入 Windows 系统后被激活的瞬间便会优先获取权限关闭杀毒软件，格式化磁盘来直接破坏计算机中的信息数据。也会篡改计算机文件数据，破坏文件的完整性并用一些“垃圾”数据来填写文件。还会进行自我复制，扩大在计算机内部的感染区域，感染其他正常文件和程序。大幅占用计算机系统运行内存和 CPU，影响计算机的正常运行，使计算机发热发烫和运行卡顿，最后导致计算机崩溃，用户数据丢失等。若在连接网络状态下，会向外发送计算机中的隐私文件，泄露个人隐私一些不法分子还会以此来向受害者索要赎金来换取文件数据。通过因特网感染大量的计算机，造成网络的瘫痪，最终对人民正常利益造成损伤。

6 Windows 系统防范计算机病毒的措施

6.1 个人用户

（1）开启 Windows 自带防护服务，选择安装有效的杀毒软件，将病毒库更新至最新版本；按时检查计算机，防止病毒感染；保证杀毒软件实时监控的开启 [2]。

（2）对于来历不明的链接或邮件，其往往会携带病毒，应慎重选择。

（3）不要执行从网站上下载的未经杀毒软件检测的程序；不要执意浏览经杀毒软件提示危险的网站。

（4）保证 Windows update 的正常使用，及时更新系统补丁。

（5）提高自身的信息安全意识，防止自己的移动设备多人使用。U 盘等移动设备在使用前应使用杀毒软件查杀病毒。

6.2 企业用户

（1）购买正版系统和安全软件。

（2）每天对企业电脑进行一次杀毒。

（3）开启安全软件的实时监控功能。

（4）培养并提高网络管理员的技术能力。

（5）当企业局域网内一台计算机遭受病毒感染时应及时切断该计算机的网络连接，防止病毒通过局域网感染其他

计算机，将损失能降低至最小。

（6）与国内知名网络公司合作，利用先进的技术保护企业计算机的安全。

（7）制定良好的管理制度，提高企业员工的计算机安全意识，加强网络信息管理，是网络管理变得更加系统化、专业化 [3]。

7 结束语

综上所述，计算机病毒看似遥远，而它就在我们身边，Windows 计算机已成为我们生活中不可或缺的一部分，对我们的生活有着不小的影响。互联网时代下计算机病毒的种类和破坏能力不容小觑。小到个人利益受损，大到社会、国家利益受损，忽略计算机病毒的危害会对我们的正常利益造成严重的影响。所以认识计算机病毒对计算机造成的危害及如何进行防范是一件非常重要的事情。

【参考文献】

[1] 沙宁，马立和 . 计算机病毒的危害和预防策略探究 [J]. 黑龙江科技信息，2014（24）:156.
[2] 唐磊 . 计算机网络安全的主要隐患及管理措施分析 [J]. 山东工业技术，2019（01）:152.
[3] 姜麒麟 . 如何做好企业计算机病毒的防范工作 [J]. 计算机光盘软件与应用，2011（12）:96.