道高一尺，魔高一丈

——计算机病毒的更新发展

16307130335　　复旦大学计算机科学与技术　　方煊杰

一、蠕虫不灭

说起蠕虫病毒，我脑海中浮现的第一个词语就是传播。

可以毫不夸张地说，任何接触过计算机的人一定接触过蠕虫病毒：来自 qq 好友突然发送的充满繁体字火星文的链接；夹杂着乱码与拉丁文字附件的电子邮件……

蠕虫病毒强大的传播能力不禁让人联想到斐波那契兔子，兔子生的兔子还可以再生兔子，如同滚雪球一般宿主飞速壮大，从而广播更多的机器。

2019 年依旧肆虐全球的 MyDoom 病毒就是一种通过邮件传播的蠕虫病毒，它是通过 SMTP(简单邮件传输协议)通过电子邮件传播的。

SMTP 是一种提供可靠且有效的电子邮件传输的协议。SMTP 是建立在 FTP 文件传输服务上的一种邮件服务，主要用于系统之间的邮件信息传递，并提供有关来信的通知。SMTP 独立于特定的传输子系统，且只需要可靠有序的数据流信道支持，SMTP 的重要特性之一是其能跨越网络传输邮件，即 “SMTP 邮件中继” 。使用 SMTP，可实现相同网络处理进程之间的邮件传输，也可通过中继器或网关实现某处理进程与其他网络之间的邮件传输。
而蠕虫用各种方法收集目标主机的信息，找到可利用的漏洞或弱点。方法包括用扫描器扫描主机，探测主机的操作系统类型、版本，主机名，用户名，开放的端口，开放的服务，开放的服务器软件版本等进行攻击传播。

多年来，MyDoon 的传播具有相同的特点。一般来说，邮件发送的是一个 MyDoom 病毒，它会伪装成一个报告发送失败后返回的报告，你会看到带有如下标题：发送失败；邮件可能无法收到等，另外，我们还经常看到 MyDoom 邮件的标题字母排列组成顺序混乱，并附带附件链接，如果点击或者下载附件 zip 包就会感染病毒。

MyDoom 恶意软件感染 Windows 主机后会将它变为恶意软件发送机器人，然后将 MyDoom 的消息发送到不同的电子邮件地址，即使被感染的 Windows 主机没有邮件客户端，它也会发送恶意消息。与此同时，MyDoom 的另一个特性是尝试通过 TCP 接口 1042，去连接多个不同的 IP 地址。

因此合理配置防火墙，禁止除需要的服务端口外的其它所有端口。由于蠕虫要通过网络感染系统，向开放的端口发送攻击代码是必不可少的一个步骤，禁止端口可以切断蠕虫的发动攻击的通道。同时，对于已经被感染的系统，防火墙也可以使它不能够再对网络中的其它计算机发动攻击。通过配置路由器，可以屏蔽和过滤含有某个蠕虫特

征的报文，达到封堵的效果。

然而虽然从 04 年就出现的古老病毒，MyDoom 依然活跃在世界各地，如同百足之虫死而不僵，确实可称一句蠕虫永不灭绝。

二、AutoRun 不绝

AutoRun 病毒，也称 U 盘病毒，其实不是什么危害性及其高的病毒，但随着时间流逝，它也因传播方便而越来越普及。

在我校学生口中，它还有另外一个名称：打印店病毒。在校内外打印店使用 U 盘后，总会发现自己 U 盘中的文件消失不见，并且之后自己的计算机似乎也会导致别人的 U 盘出现同样的问题。

U 盘病毒事实上是通过向 U 盘写入病毒程序，然后更改 autorun.inf 文件。autorun.inf 文件记录用户选择何种程序来打开 U 盘。如果 autorun.inf 文件指向了病毒程序，那么 Window 就会运行这个程序，引发病毒。一般病毒还会检测插入的 U 盘，并对其实行上述操作，导致一个新的病毒 U 盘的诞生。

U 盘病毒都是通过 Autorun.inf 来进入的；Autorun.inf 本身是正常的文件，但可被利用作其他恶意的操作；不同的人可通过 Autorun.inf 放置不同的病毒，因此无法简单说是什么病毒，可以是一切病毒、木马、黑客程序等；一般情况下，U 盘不应该有 Autorun.inf 文件；如果发现 U 盘有 Autorun.inf，且不是你自己创建生成的，请删除它，并且尽快查毒；如果有貌似回收站、杀毒文件等文件，而你又能通过对比硬盘上的回收站名称、正版的杀毒软件名称，同时确认该内容不是你创建生成的，请删除它。

同时，一般建议插入 U 盘时，不要双击 U 盘，另外有一个更好的技巧：插入 U 盘前，按住 Shift 键，然后插入 U 盘，建议按键的时间长一点。插入后，用右键点击 U 盘，选择 “资源管理器” 来打开 U 盘。

三、勒索永存

马克思曾说过：“如果有 10%的利润,它就保证到处被使用；有 20%的利润,它就活跃起来；有 50%的利润,它就铤而走险；为了 100%的利润,它就敢践踏一切人间法律；有 300%的利润,它就敢犯任何罪行,甚至绞首的危险” 。

这也是勒索病毒逐渐兴起并成为计算机新型高危病毒的原因。很多别的病毒大多为了植入木马操控电脑，更多偏向搜集信息；而勒索病毒顾名思义则意味着获得实质的利益。

首次出现在 2019 年 5 月的 Buran 病毒，是一款新型的基于 RaaS 模式进行传播的新型勒索病毒，在一个著名的俄罗斯论坛中进行销售， Buran 勒索病毒此前使用 RIG Exploit Kit 漏洞利用工具包进行传播，其利用了 Internet Explorer 的一个比较严重的漏

洞 CVE-2018-8174，近期发现此勒索病毒利用 IQY(Microsoft Excel Web 查询文件)进行传播。

勒索病毒文件一旦被用户点击打开，会利用连接至黑客的 C&C 服务器，进而上传本机信息并下载加密公钥和私钥。然后，将加密公钥私钥写入到注册表中，遍历本地所 有磁盘中的 Office 文档、图片等文件，对这些文件进行格式篡改和加密;加密完成后，还会在桌面等明显位置生成勒索提示文件，指导用户去缴纳赎金。

该类型病毒可以导致重要文件无法读取，关键数据被损坏，给用户的正常工作带来了极为严重的影响。

主要特点是通过自身的解密函数解密回连服务器地址，通过 HTTP GET 请求访问加密数据，保存加密数据到 TEMP 目录，然后通过解密函数解密出数据保存为 DLL，然后再运行 DLL (即勒索者主体)。该 DLL 样本才是导致对数据加密的关键主体，且该主体通过调用系统文件生成密钥，进而实现对指定类型的文件进行加密，即无需联网下载密钥即可实现对文件加密。

计算机病毒多种多样，但来源归根结底还是不安全的链接，未加证书的网页等，只要我们能够保持谨慎，不轻易访问未知链接，善用防火墙，那么在大多数情况下还是可以保证自己计算机的安全。