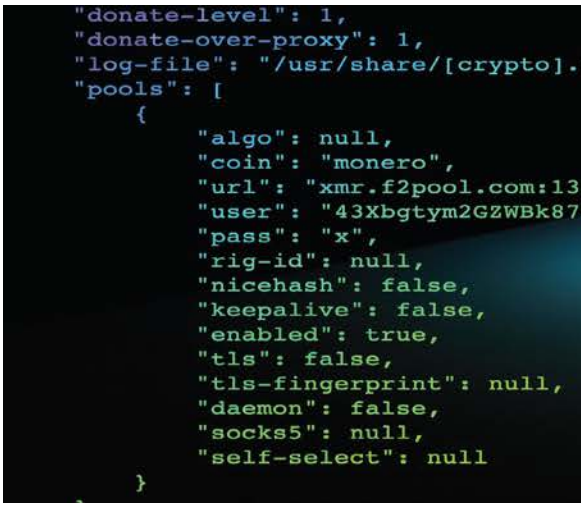
黑客入侵与防护

随着互联网应用的普及，网络给人们带来生活、工作上的便利，信息丰富、多元化的同时，也存在着极大的安全隐患。近年来，全球各地和各个国家，黑客入侵政府网站、企业后台，篡改和盗取重要数据，并以此进行威胁、勒索，以达到获取经济利益的事件，屡见不鲜。针对网络安全问题，如何进行有效的防范，令许多政府机关、企业网站，感到非常头痛、棘手。



黑客攻击常见的方式有五种:

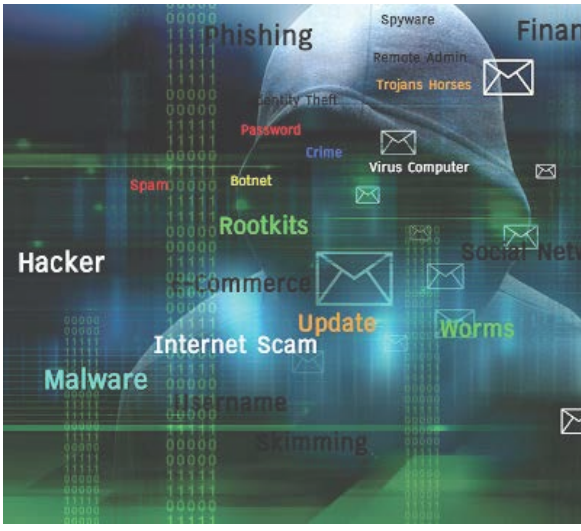
第一种是"钓鱼网站"

攻击方式：这是一种比较常见的作案手法，黑客会模仿一些知名钱包网站，交易所，项目官网，域名也极其相似，比如将后缀从标准的.com变成.cn或.io等。网银大盗Ⅱ（Trojan/KeyLog.Dingxa）木马程序。

个案分享：在2004年6月再次发现新变种病毒，非主动传播，主要通过用户在浏览某此网页或点击一些不明链接或打开不明附件等操作时，间接感染用户电脑，不但给染毒用户造成的损失更大，更直接，也给各网上银行造成更大的安全威胁和信任危机。2018年8月台湾某大型制造业工厂在安装新机台时，因没有按照操作流程，遭受WannaCry的变种病毒感染，病毒入侵至集团内三处重要生产机地，生产线全数停摆几个小时，损失为25.96亿，约占季营收1%。

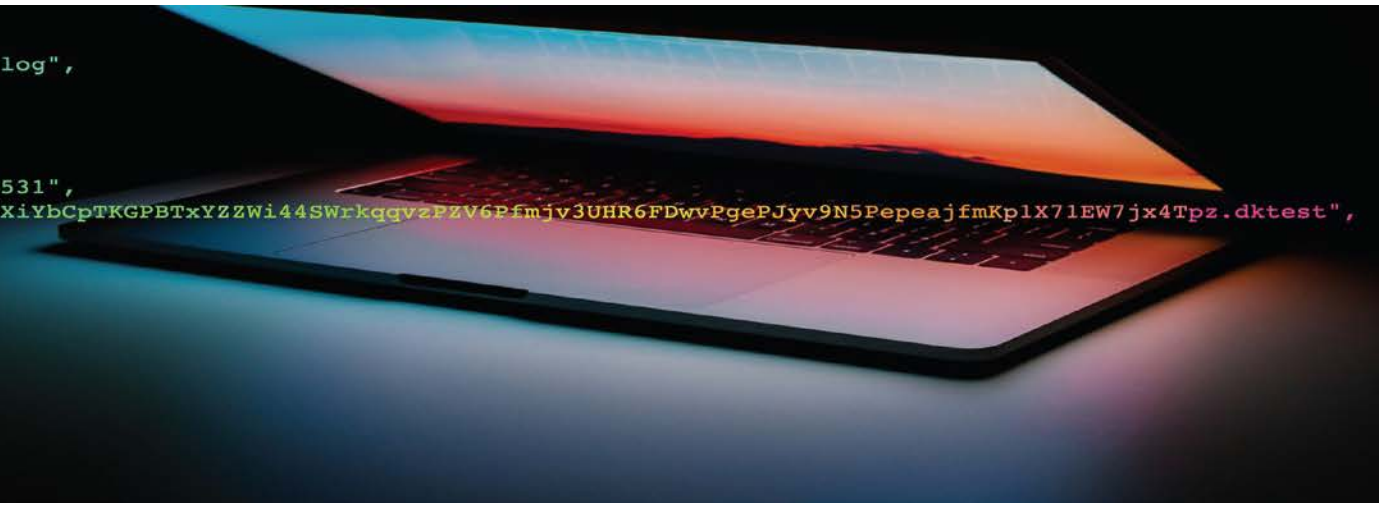
防护方法：避免使用别人在群里转发的地址，直接在百度搜索官网地址。

第二种是“邮件传输”



攻击方式：在互联网上，人们永远不应该点击他们不知道或不关心的链接。不幸的是，最近几年发生了完全相反的情况。同样的道理也适用于那些看起来可疑的电子邮件附件。最好的做法是完全忽略这些，然而事实证明做到这一点是困难的。特别是在公司环境中，电子邮件附件似乎是随意下载的，因为工作中职工往往担心错过了关键信息。

越来越多的恶意电子邮件附件也带来了新的威胁。加密劫持和勒索软件恶意软件通常通过电子邮件传播。同样的道理也适用于木马和犯罪分子部署的其他类型的恶意软件。当电子邮件中存在附件时，务必验证一下发件人，不要随意点击打开。如果是未知来源，请不要下载附件将其发送给公司的安全团队，凭这一点就能避免很多问题。电子邮件作为信息的承载体，其面临的安全保密威胁主要就是邮件被截获，邮件内容外泄，以及邮件附件携带病毒（如勒索病毒、邮件蠕虫My Doom等）。导致电脑重要数据或被盗，或损坏以及造成网络、服务器瘫痪。



个案分享：番禺某小学“法伦功”反动宣传的电子邮件堵塞网络安全事件；深圳市二十多个服务器转发匿名电子邮件转发事件。
防护方法：不要随便打开来源不明的附件或连接，遇到任何怀疑，请先找IT确认。

第三种是对公司“防火墙”进行攻击
攻击方式：防火墙能极大地提高一个内部网络的安全性，并通过过滤不安全的服务而降低风险。也正因为他具有将内部网和公众访问网（如Internet）分开的方法，是一种建立在现代通信网络技术和信息安全技术基础上的应用性安全技术，隔离技术。所以他的薄弱点也正是黑客入侵的主要对象，多通过预攻击行为和端口渗透还有系统漏洞进行攻击。

个案分享：深圳某企业网安人员2019年6月期间经常截获一些非法数据包，这些数据包多是一些端口扫描、SATAN扫描或者是IP半途扫描，扫描时间长，间隔时间短，每天持续10~20次左右。于是网安人员初步判定公司网络已经被盯上，并及时采取加固网络，同时反向追踪扫描地址，并给予了扫描者一个警示信息。以使攻击行为未尝所愿，最终停止攻击此公司的行为。

防护方法：针对以上黑客日新月异的攻击方式。公司采用了主流防火墙产品及上网行为管理系统相结合，做到事前防护，事中控制，事后审计。公司通过部署防火墙，极大地提高公司内部网络的安全性，并通过过滤不安全的服务而降低风险；通过防火墙对内部网络的划分：办公网、生产局域网、特殊敏感网段、客户网，实现内网重点网段的隔离，从而限制了局部重点或敏感网络安全问题对全局网络造成的影响。将大部分的外部入侵安全事故降到最低，最大限度阻止网络中的黑客访问公司的网络。

公司还引入了上网行为管理系统及其它工具，将可能带来风险的移动存储，及传递风险的邮件系统，以及公司电脑对各个知名网站的访问进行监控，及时发现异常，并处理。如2021年4月初邮件警示：一些不法分子冒充公司高层邮箱发送邮件，获取公司信息，但因公司人员警觉性高和立即邮件通告，以及IT后台及时处理防范，将可能的冒充邮箱列入黑名单，而未造成公司损失。公司内还采取对所有在用移动存储要求登记备案，随时监控，以预防不安全事件发生。公司通过在上网行为管理系统上做设定，限制相关网站的访问，及上传下载，包括流量管控，以防止钓鱼网站有可乘之机等等。总之为了打造一个信息安全的公司内部网络，为了“满足客户要求，实施风险管理，确保信息安全，实现持续改进”，我们不断的从硬件、软件系统，以及人员的意识一步步完善。

黑客入侵 与防护

第四种是破解密码

攻击方式 ： 人们被黑客攻击的主要原因还是他们自己的密码操作。使用过于简单的密码，通常情况下简单密码很快便会被破解出来，这几乎是很多消费者和企业会出现的问题。这类情况一般可通过密码管理器来生成独特的组合。

通常，重复使用同一个密码也是一种不好的做法。如果黑客以某种方式获得站点a的登录凭证，那么同样的组合很可能也适用于站点B、C、D和E。这就给犯罪分子留下了大量的个人信息，他们可以利用这些信息，而这些信息在任何时候都需要避免。

个案分享：依照惯例，“飞溅数据”通过分析今年黑客张贴在网上的数百万个被盗用户名和密码，整理出这份榜单，并参考历年资料，为排名增加了“走势变化”。上榜的25个密码大多有规律可循，多为键盘上的相邻键组合或常见名称，比如由键盘上位置相邻的字母组成的qwerty排名第五。常见数列111111、123456、123123及一些常用名字，如ashley、michael等均榜上有名。

防护方法：密码十位数以上，数字+英文+符号,及不用连续号码或英文名字

第五种是远端操纵

攻击方式：远端操纵是指黑客在目标计算机中启动一个可执行程序，该程序将会显示一个伪造的登录界面，当用户在该界面中输入账户、密码等登录信息后，程序将用户输入的账户、密码传送到黑客的计算机中。同时程序关闭登录界面，提示“系统出现故障”信息，要求用户重新登录。这种攻击类似于在Internet中经常遇到的钓鱼网站。

个案分享：美国一名“黑客”高手在洛杉矶遭逮捕。他被控利用“远程黑客控制网络”操纵他人电脑系统，并散发大量广告信息，以此赚取非法收入。美国联邦检察官发言人汤姆·姆罗策克说，被捕黑客名叫简森·詹姆斯·安切塔，现年20岁，是地下黑客组织“BOT（机器人程序）大师”的著名成员。“远程黑客控制程序”也叫机器人程序，在通过网络秘密安装进个人电脑后，黑客就可以利用该程序控制被入侵的电脑。“远程黑客控制网络”则是由数以千计的受这种程序控制的电脑组成，黑客可利用这一网络实施大规模网络攻击，或散发大量垃圾邮件和广告信息。

防护方法：不要随便打开来源不名的附件、链接、不安装不明来源的软件及更新系统补丁。

撰文：Harry（信息技术部）