常见病毒攻击摘要

一、黑链

黑链，是指看不见，但是却被搜索引擎计算权重的外链，也叫暗链。主要是黑客用非正常的手段获取其它网站的反向链接。最常见的黑链就是通过各种网站程序漏洞获取搜索引擎权重较高网站的webshell，进而在被黑网站上链接自己的网站，其性质与明链一致，都是属于为高效率提升排名，而使用的作弊手法。黑链最常用的潜伏方式就是通过控制CSS属性隐藏。

通常来讲，受害主机存在以下两个明显的危害：  
1、组织单位社会形象严重受损  
存在漏洞的搜索引擎权重或者PR较高的网站容易被植入博彩、色情、游戏等黑链，当访问者点击被挂黑链网站时，会被引导到相关的博彩、色情网站，使组织单位的社会形象受损，网站运营者甚至要承担相应的法律责任。  
2、严重影响网站的推广  
被挂黑链网站由于存在太多单向链接，会造成网站快照更新慢、网站排名下降等问题。而网站一旦被搜索引擎发现黑链行为，会被降权或者从关键词排名剔除，非常损害网站的推广。  
同时，黑链已经被植入受害主机，表明主机很可能已被黑客控制，现有的安全防护体系已经部分甚至完全失效，还存在以下潜在风险：  
1、组织单位遭受更进一步的损失  
攻击者可以进一步对网站实行挂马、信息篡改、信息窃取和信息监控，严重威胁用户网站的安全，导致企事业单位遭受更进一步的资产损失。  
2、遭受监管单位通报  
黑客将恶意程序植入受害主机，控制主机作为“肉鸡”攻击互联网上的其他单位，违反网络安全法，遭致网信办、网安等监管单位的通报处罚。

通常来说，被挂载了黑链的主机可以确定当前业务系统已经被攻破，是极其严重的安全事件。而要想完全解决黑链问题，是一个系统性的工程，我们按照清除黑链、事件溯源、清除恶意软件、安全加固等方面来进行阐述。