

在武侠小说中有这样一类人，他们武功高强，却又不愿走正统建功立业的英雄之路，于是劫富济贫为民请命，解救劳苦平民大众于水火之中，这类人被称为“侠盗”。而在病毒界，GandCrab勒索病毒凭借之前将叙利亚以及其他战乱地区加进感染区域白名单的“侠义”行为，也博得了很多好感，不少人称呼其为“侠盗病毒”。

## 瞄准国内政企高校

## 意图实现全垒击打

不过，这个“侠盗病毒”志不在“侠”，它的全部精力可都用在了“盗”上。这不，近期360安全大脑就监测到GandCrab v5.2正大肆攻击巴西、美国、印度、印度尼西亚和巴基斯坦等多个国家，大有向着2017年WannaCry病毒“昔日荣光”进发的迹象。



不过广大用户以及管理员不必惊慌，360安全卫士已经实现了对GandCrab勒索病毒4.0/5.0/5.0.2/5.0.3/5.0.4/5.1版本的解密，并全面支持针对GandCrab勒索病毒全系列的强力查杀。装有360安全卫士的电脑用户，能有效防御GandCrab的攻击，绝无中招之患！

## 不停升级“传送门”

## 开启暗网代理新模式

作为病毒界一颗冉冉升起的“勒索新星”，GandCrab勒索病毒自2018年面世之初便快速增长，国内不少Windows服务器上的文件被加密。发展势头之迅猛在其不断升级的传播方式上就可见一斑——曾使用U盘蠕虫、下载器、远程桌面爆破、永恒之蓝漏洞、网页挂马等各种方式传播，最近更是迷上了邮件攻击。

攻击者通过向受害人发送虚假邮件，引导用户下载打开邮件中的不明附件，随后便立刻加密受害者主机硬盘数据，以此要求受害者支付赎金。



此外，针对该勒索病毒的攻击感染态势，360安全大脑提醒广大政企用户要做好以下防护措施：

- 1、安装360安全卫士，对GandCrab勒索病毒进行防御和强力查杀，全方位保护个人数据和财产安全；
- 2、提高安全管理意识，关闭不必要的端口和共享文件；
- 3、及时给系统安装补丁，修复服务器系统、Web应用漏洞，使用强度高的服务器登录口令与Web应用后台登录密码，防止攻击者通过漏洞利用或弱口令爆破等方式攻击服务器；
- 4、切记不要輕易点击来历不明的邮件，企业邮件服务器可尝试部署邮件安全网关、升级安全策略，将此类邮件拉入垃圾邮件黑名单等措施实施防御。

来源：消费日报网