# 黑客勒索病毒防治工作总结(推荐3篇)

来源：网络 作者：逝水流年 更新时间：2024-07-25

*黑客勒索病毒防治工作总结1勒索软件具有强破坏性。一旦运行起来，用户很快就会发现其特征，如部分进程突然结束、文件不能打开、文件后缀被篡改、屏保壁纸被更换等。7. 物理隔离强制关机和关闭网络关闭网络包括拔网线、禁网卡，笔记本禁用无线网络 访问控...*

**黑客勒索病毒防治工作总结1**

勒索软件具有强破坏性。一旦运行起来，用户很快就会发现其特征，如部分进程突然结束、文件不能打开、文件后缀被篡改、屏保壁纸被更换等。

7. 物理隔离

强制关机和关闭网络

关闭网络包括拔网线、禁网卡，笔记本禁用无线网络

访问控制

加策略防止其他主机接入，关闭感染主机开放端口如445、3389等，修改感染主机及同局域网下所有主机密码，密码采用大小写字母、数字、特殊符号混合的长密码。

确认损失

查看感染主机数量，根据感染特征，排查未感染主机，统计受损情况并列出清单。

主机加固

对未受感染主机进行加固处理，包括：

登录密码采用强密码(大小写字母、数字、特殊符号混合，长度为15+)

更新系统补丁，更新应用软件到最新版本

保护现场

当以上措施结束之后，尽量不要再操作受感染主机，等待相关专业人员进行处理。

当数据被加密，如何对数据进行恢复。一般情况数据恢复有以下途径。

备份恢复

利用备份数据恢复是当前数据恢复途径中最有效且成本最低的恢复方式，所以如果在固定的工作周期及时进行备份，这时就可以轻松应对。但是在恢复时一定要注意将被感染机器的勒索病毒清除干净，最好是格式化磁盘或者重装系统并及时修复系统漏洞，保证安全之后再恢复备份，防止二次感染。

7. 解密工具

利用网上提供的解密工具进行修复，在一些特定情况下，如勒索软件通过读取文件副本加密然后删除原文件的方式，如果原文件内存未被覆盖，或者勒索软件尚未加密完成，及时发现后强制关机。部分文件未加密，这些情况都有几率成功恢复。

也可以使用很多在线解密网站的解密工具。通过公开的密钥进行解密，其密钥获取主要的方法为以下四种方法：

1.勒索软件本身算法存在缺陷，内存中可找到密钥；

2.攻击者服务器比较脆弱，通过攻陷服务器，获取解密密钥；

3.多国联合执法，通力合作，抓捕攻击者获取密钥并公开发布；

4.攻击者自己良心发现，公开密钥。

7. 支付赎金

如果加密数据过于重要且无法免费解密，不得不缴纳赎金时，也需要注意，因为有部分勒索软件本身存在缺陷无法进行解密，即使缴纳赎金也无法恢复。另外一般赎金的类型为加密货币如比特币、达世币等，与法币交易不同，最好是找相关的安全专家进行综合判断之后，再确定是否缴纳赎金。不然如果盲目交钱，很可能最后人财两空。

重装系统

如果数据不重要或者通过上述方法解密成功并对数据做好备份之后，一定要重装主机系统，及时更新补丁等，防止二次勒索。

**黑客勒索病毒防治工作总结2**

20\_年9月，欧洲国家黑山的多个政府部门遭遇超大规模网络攻击，致使超过10个政府机构的150多个工作站均无法访问。此次攻击采用了勒索软件与分布式拒绝服务（DDoS）相结合的方式，不仅扰乱了政府服务，还迫使该国的电力系统转为手动控制。

>

黑山国家\_将这起在上周末发起的攻击直接归因于俄罗斯，但没有给出任何证据。有一个勒索软件团伙宣称对此次攻击至少负部分责任，他们使用Cuba勒索软件感染了黑山议会办公室。网络安全公司Profero的调查显示，该团伙中有成员使用俄语，同时Cuba勒索软件在勒索门户上也发布了黑山议会勒索公告，称窃取了财务文件、银行通信内容、资产负债表、税务文件、赔偿金乃至源代码。这些文件免费发布，任何人均可下载。

《每日邮报》9月25日报道称，有人在论坛上爆料称，黑客正在勒索澳洲第二大电信运营商Optus，要求对方支付价值153万澳元的加密货币，否则就出售被盗的用户信息。

C114资讯北京时间9月27日报道，一个名为“optusdata”的在线论坛账号为黑客账号持有人发布消息称，由于“关注的人太多”，他们已经删除了数据，并撤回了赎金要求，同时对已经泄露了万名澳大利亚人的数据表示抱歉。

Optus发表声明称，用户密码和财务信息没有泄露，但姓名、地址、出生日期、电话号码、驾照以及护照信息可能泄露。

澳大利亚联邦政府将此次网络入侵归咎于Optus，提出了隐私法规的全面改革和更高的罚款，并指出该公司“实际上为黑客窃取数据留下了方便之门”。

>10月份

**黑客勒索病毒防治工作总结3**

据BleepingCompuer11月3日消息，知名勒索软件组织LockBit宣布他们对德国跨国汽车集团大陆集团（ Continental） 发动了网络攻击。LockBit声称，他们窃取了大陆集团系统中的一些数据，如果不能在11 月 4 日 15:45:36（北京时间23:45:36）之前收到赎金，他们将在数据泄露网站上公开这些数据。

目前LockBit尚未透露赎金的具体金额，以及窃取数据的具体时间及其他任何细节，但由于显示支付赎金的倒计时页面仍在刷新，表明大陆集团还尚未与勒索软件进行谈判，已经决定拒绝支付赎金。

今年8月，大陆集团系统曾遭到过攻击者入侵，事后公司声称立即采取了所有必要的防御措施，并在外部网络安全专家的支持下，对事件进行调查，公司业务没有受到任何影响。BleepingCompuer向大陆集团 询问这起事件是否和此次LockBit的勒索攻击相关，大陆集团美国公司传播与营销副总裁 Kathryn Blackwell 给出了否定的回复，并称无法提供更进一步的任何细节。

LockBit 勒索软件于 20\_ 年 9 月作为勒索软件即服务(RaaS) 首次出现以来，已经制造多起重大勒索攻击事件。就在今年，LockBit 曾分别向意大利国税局和安全巨头Entrust发动过勒索攻击。

本文档由站牛网zhann.net收集整理，更多优质范文文档请移步zhann.net站内查找