360安全卫士的文档保护功能

敲诈者病毒如此蛮横且疯狂，360却有妙招对付它。就算敲诈者病毒“心机颇深”采用各种伪装等技巧躲避杀软，360安全卫士依然能识别并拦截各类敲诈者病毒及其变种。还能够在遇到可疑程序篡改文档时，自动识别并弹窗提醒，保护文档安全。360安全卫士在新版本11.0中还推出了“反勒索服务”，并同时提供一站式服务，协助解锁加密文件。

主要通过邮件附件传播，针对有钱人

由于是进行私人文件加密，CTB-Locker传播对象主要为企业高管或有钱人，主要通过邮件附件进行传播，并针对特定人群进行精准投放。硬盘有价，数据无价，对于许多企业和个人用户而言，数据丢失将是难以承受之重，而比特币敲诈者正是瞄准了这一市场。病毒作者遭到曝光，但随后支付环节使用TOR等代理进行中转，始作俑者波格契夫凭借终结者宙斯以及比特币敲诈者两种病毒就令12个国家超过一百万计算机感染，经济损失超过1亿美元。

勒索病毒攻击原理是什么

2017年5月12日，WannaCry蠕虫通过MS17-010漏洞在全球范围大爆发，该蠕虫感染计算机后会向计算机中植入敲诈者病毒，导致电脑大量文件被加密。受害者电脑被黑客锁定后，2017年5月13日晚间，研究人员分析此次勒索软件时，而是直接删除。实现了部分文件恢复。2017年5月14日，监测发现，WannaCry勒索病毒出现了变种：WannaCry2.0，这个变种取消了，该变种传播速度可能会更快。请广大网民尽快升级安装Windows操作系统相关补丁，已感染病毒机器请立即断网，避免进一步传播感染。勒索病毒攻击类型

表现形式

通过设置电脑开机密码、登录密码等对电脑锁屏，比如WinLocker、PCCyborg、敲竹杠木马等，会采用锁定系统屏幕等方式，迫使系统用户付款，通过威胁恐吓用户，实施敲诈：比如FakeAV敲诈者病毒会伪装成反病毒软件，诱骗用户付款购买其“反病毒软件”。声称用户触犯法律，迫使用户支付赎金。2015年，加密用户用户文件和数据，要求支付赎金：加密用户文档，只有在用户支付赎金后，VirLock、Locky等敲诈者病毒也都是这个类型。由于病毒对文档采用RSA等高强度非对称加密，一旦中招就无法恢复，除非给黑客交赎金购买解密密钥。篡改磁盘MBR，制造计算机蓝屏重启，之后加密电脑整个磁盘敲诈赎金：使Windows崩溃并显示蓝屏，而当用户重启计算机时，加密整个磁盘，之后显示一个ASCII骷髅图像，而且因为修改MBR，所以容易防御。

勒索病毒善伪装造成的破坏不可逆

金山公司反病毒专家李铁军告诉记者，诸如比特币木马等勒索类病毒近来比较常见。也就是说，除了病毒开发者本人，”。勒索类病毒通常通过电子邮件传播，诱导电脑用户打开文档。病毒程序就可能运行。”李铁军说，我们分析过，”李铁军说，很多黑客进行改造，开发出更多病毒变种”。

传播感染背景

本轮敲诈者蠕虫病毒传播主要包括Onion、WNCRY两大家族变种，本次感染事件首先在英国、俄罗斯等多个国家爆发，新闻报道有多家企业、损失非常惨重。安全机构全球监测已经发现目前多达74个国家遭遇本次敲诈者蠕虫攻击。从5月12日开始，在多个高校和企业内部集中爆发并且愈演愈烈。1.全球74个国家遭遇Onion、漏洞编号:MS17-010)。“冲击波”等大规模蠕虫感染类似，传播感染速度非常快。但是在教育网、对于企业来说尤其严重，从我们检测到反馈情况看，国内多个高校都集中爆发了感染传播事件，甚至包括机场航班信息、加油站等终端系统遭受影响，