病毒概况

进行网络端口扫描攻击，目标机器被成功攻陷后会从攻击机下载WannaCry病毒进行感染，并作为攻击机再次扫描互联网和局域网其他机器，形成蠕虫感染，大范围超快速扩散。病毒母体为mssecsvc.exe，尝试感染，会释放敲诈者程序tasksche.exe，对磁盘文件进行加密勒索。病毒加密使用AES加密文件，并使用非对称加密算法RSA2048加密随机密钥，每个文件使用一个随机密钥，理论上不可破解。

“天杀的马斯克”

给同事发去这么一句。这是他人生中第一次买入数字货币。只是听说马斯克要在一档节目上聊起狗狗币，他就觉得一定会大涨，在区块链信息平台巴比特论坛上，“世界首富都站台”、“干死灰度”，他们发帖说。狗狗币在早期就被当作论坛币在reddit打赏。在今年4月中旬，reddit网友开始集结在WSB板块，与华尔街就GameStop股价多空博弈时，马斯克当时发推特说。

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。

查封恶意程序来源，查杀恶意程序落地和调用，确保勒索病毒不会被运行。

360防御勒索病毒武器NO.5——360文档卫士：360文档卫士作为“勒索病毒终结者”，实时全面保护文档安全，具有自动备份引擎，发现文档修改后自动备份，做到有备无患。360文档卫士还提供了文档解密功能，一键扫描中了什么勒索病毒，直接推荐解密工具，360防御勒索病毒武器NO.6——反勒索服务：360安全卫士独家开通“反勒索服务”，使用360安全卫士11.0版本并开启该服务后，一旦感染敲诈者病毒，

敲诈者

一种比特币敲诈病毒席卷国内高校校园网，导致用户电脑被锁，许多实验室数据和毕业设计被加密，许多网友纷纷发帖向腾讯电脑管家求助如何才能解救中招电脑。该木马通过加密形式，导致用户无法正常使用程序。腾讯电脑管家提醒：一定要保持腾讯电脑管家开启状态。#敲诈者#标签聚合页面仍在完善中，后续将为您提供丰富、#敲诈者#图片信息、视频内容，小编将持续从百度新闻、搜狗百科、微博热搜、知乎热门问答以及部分合作站点渠道收集和补充完善信息。