

# 勒索病毒让全球“想哭”，谁之过

不光是美国政府和发动袭击的黑客，疏于防范的“中招”者也难辞其咎

一个名为“想哭”的勒索病毒12日以来袭击全球150多个国家和地区，影响领域包括政府部门、医疗服务、公共交通、邮政、通信、汽车制造业等。

在遏制病毒扩散的过程中，人们开始反思：这场突如其来的灾难，究竟是谁之过？

## 责怪对象之一：美国政府

包括美国微软公司、Splunk网络安全公司在内，业界普遍共识是：“想哭”病毒来源于美国国家安全局的病毒武器库。上个月，美国国安局遭遇泄密事件，其研发的黑客攻击工具被公之于众。

美联社评论，这次席卷全球的袭击中，黑客并非独立研发出“想哭”病毒，因此美国国安局难辞其咎。

不少人指责，美国政府察觉到微软安全漏洞，却没有及时告知微软公司，反而囤积攻击工具，以致泄露后祸及全球。美国公民自由联盟呼吁国会通过立法，以强制美国政府及时向IT企业通报安全漏洞，以便这些公司及时采取补救措施。

此外，一些网络安全专家批评，美国斥巨资研发黑客攻击工具，而非自卫机制，结果造成全球网络环境“更不安全”。美国联邦政府公布的数据显示，美国网络项目开支中，90%用于研发黑客攻击武器。

美国高德纳咨询公司网络安全分析师阿维瓦·利坦说，美国政府确实“存在疏忽”。但他对此感到无奈，“我们无法阻止美国政府研发网络攻击武器”。



▲5月15日，在德国法兰克福火车站，乘客经过恢复正常的列车电子时刻表。此前，这里曾遭到网络病毒袭击。

## 责怪对象之二：微软公司

“想哭”病毒利用微软“视窗”操作系统漏洞发动攻击，微软公司由此受到抨击。

利坦认为，微软已于3月发布针对此类勒索软件的补丁，凡是安装过补丁的用户不太可能遭受这款病毒攻击。但是，微软提供的补丁只针对新版本的操作系统，而并不包括“Windows

XP”等较老版本。直到本月12日全球电脑纷纷“中招”后，微软才宣布为较老版本的操作系统的免费提供补丁。

本轮病毒攻击中，一些国家的医院系统、公共交通系统发生瘫痪，而这些部门往往出于财务考虑而一直沿用“Windows XP”。观察人士表示，如果某机构受限于财务状况，没有使用新版本的视窗系统，自然也就不太可能付费打补丁，而这些本应由

微软公司考虑到。

## 责怪对象之三：“中招”者

一些网络安全专家认为，这次病毒攻击虽然影响范围广，但是从技术而言并不难防范。只要及时安装更新包，修复电脑操作系统漏洞，便不会轻易“中招”。

利坦说，医院系统、政府部门应对联网电脑进行更妥善的保护，例如限制登录网站、限定运行软件的权限、只授权专门技术人员进行某些操作等。

此外，这类部门还应对所存储的文件做好备份。在此次勒索软件袭击中，如果“中招”者拥有备份，就无需支付赎金来挽回文件。

## 责怪对象之四：黑客

眼下，美国、英国、俄罗斯等国都在追查这次袭击的幕后黑手。

中毒电脑上会弹出勒索信息，提示电脑用户在规定时间内支付300美元赎金；每耽搁数小时，赎金额度就会上涨一些，最高涨至600美元。据观察，一些用户使用虚拟货币比特币支付了赎金。

美联社报道，截至15日，黑客已收到大约7万美元的赎金。一名不愿公开姓名的美国高级官员透露，美国总统唐纳德·特朗普12日晚下令召集一次紧急会议，联邦调查局、国安局随后联手展开调查。据路透社报道，相关调查都在初始阶段，而锁定黑客身份的难度相当大。

(记者杨舒怡)据新华社专特稿

# 卡巴斯基谈防毒解毒：下正规“补丁”，别贸然解密

勒索病毒所使用的加密算法非常严密，目前已知的解密方法都对其无效。贸然下载的解密程序可能对中毒电脑和与其联网的电脑有潜在危害，甚至加速勒索病毒传播

新华社莫斯科电(记者栾海)俄罗斯卡巴斯基实验室15日在接受新华社记者采访时表示，及时下载正规补丁程序，确保全面启用最新升级的防护软件，可防止名为“想哭”(Wanna Cry)的勒索病毒侵入电脑。但如果电脑已被这种病毒感染，目前只能重装系统来继续使用电脑，被“绑架”的文件将会丢失。

卡巴斯基实验室新闻处向记者提供的一份声明说，这种勒索病毒可通过互联网，利用微软操作系统的服务器消息块协议的MS17-010漏

洞潜入电脑，并在电脑中安装恶意驱动程序，对染毒电脑中的文件加密，以勒索“赎金”。

卡巴斯基运用其电脑系统监测工具，找到了迄今这种勒索病毒对用户文件进行加密的11种恶意程序。

卡巴斯基的专家指出，假如用户发现其电脑中的文件已被恶意加密，千万不要用各种网站上流传或电子邮件主动提供的工具程序去解密。勒索病毒所使用的加密算法非常严密，目前已知的解密方法都对其无效。贸然下载的解密程序可能对中毒电脑和与其联网的电脑有潜在危害，甚至加速勒索病毒传播。

卡巴斯基认为，预防是对付这种勒索病毒的重中之重。人们应尽快下载微软公司提供的修复MS17-010漏洞的“视窗”(Windows)操作系统补丁程序，为电脑安装技术可靠的安全监测软件并升级到最新版本，使监测软件的各项防护功能“火力全开”，尤其要让该软件的系统扫描功能处于自动工作状态，以减少勒索病毒侵入电脑的风险。

卡巴斯基建议各单位的网络管理员还需运用各种网络防护方案，确保本单位内网的所有网络节点都处于严密监护下。一旦监测软件发现上述11种恶意程序中的任何一种已经渗透进电脑，只能立即切断染毒电脑与互联网和单位内网的连接，备份尚未被恶意加密的文件，然后重装电脑系统。

卡巴斯基指出，其专家发现少数没有使用微软操作系统，不存在MS17-010漏洞的电脑也会被勒索病毒攻陷，其原因待查。但相比较而言，操作系统中存在上述漏洞的电脑显然更容易“中招”。

据卡巴斯基介绍，目前技术先进的一些防毒软件能在勒索病毒躲过各种常规防护手段、刚开始修改电脑硬盘文件时，立即阻止这种改动，为用户抢救文件争取更多时间。

目前包括卡巴斯基在内的网络安全公司正在开发更有效抵御勒索病毒、对遭受恶意加密的文件进行解密的技术手段，一旦研发成功，就会及时发布信息。

## 病毒感染啥症状，国内用户怎么防

据国家互联网应急中心博士、工程师韩志辉介绍，“被该勒索软件入侵后，用户主机系统内的照片、图片、文档、可执行程序等几乎所有类型的文件都将被加密，加密文件的后缀名被统一修改为‘.WNCRY’，并会弹出勒索对话框，要求受害者支付价值数百美元的比特币；且赎金金额还会随着时间的推移而增加。”

国家互联网应急中心建议用户及时更新Windows发布的安全补丁，在网络边界、内部网络区域、主机资产、数据备份方面关闭445、135、137、139等端口(可认为是计算机与外界通讯的出口)的外部网络访问权限，加强这些端口的内部网络区域访问审计，及时发现非授权行为或潜在的攻击行为；安装并及时更新杀毒软件；不要轻易打开来源不明的电子邮件；并定期在不同的存储介质上备份信息系统业务和个人数据。(记者王思北、李亚红)据新华社北京电

# 手机安全风险报告出炉，你的移动支付安全吗

在移动支付成为主流支付方式的当下，诈骗短信将“魔爪”伸向了支付与理财

从5月11日至31日，互联网安全公司360将在全国21个城市推广“手机安全日”系列活动，以提升全国各地手机用户的安全意识。在“手机安全日”活动期间，360发布了《2017年中国手机安全风险报告》。

报告显示，2016年中国移动支付总额约209万亿元，手机正成为个人财富中心，然而移动支付安全状况却不容乐观。93%的钓鱼网站、34.8%的恶意程序威胁个人财产。去年，猎网平台共收到全国用户提交的网络诈骗举报，涉案金额高达1.95亿元。

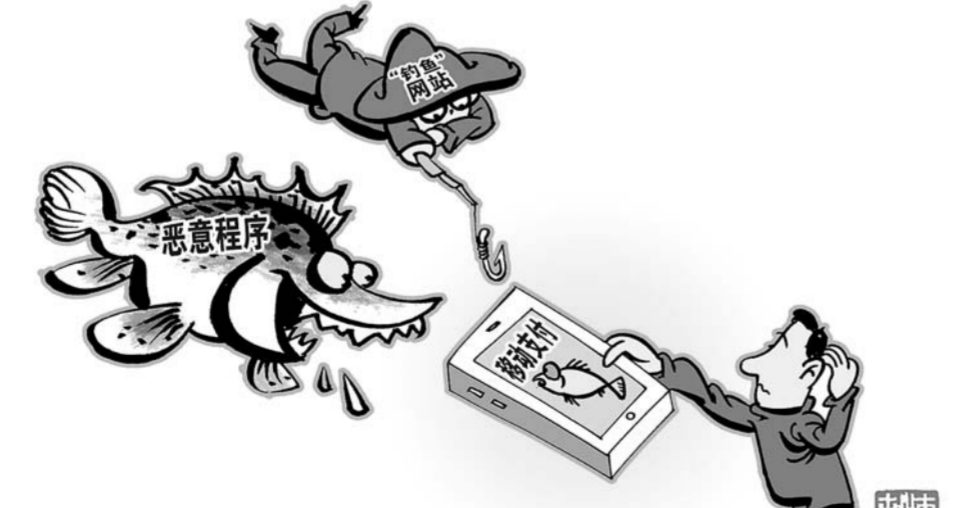
随着移动互联网和智能手机的发展，人们使用钱包和现金的机会越来越少，用手机支付的比例却越来越高。同时，各种窃取财产的诈骗手段也如影随形，恶性案件层出不穷。

360集团助理总裁、手机卫士业务负责人姚彤表示，移动支付时代，手机不仅是个人钱包和私人银行，更是个人的财富中心、信息中心、社交中心和生活中心。但一些公众仍然缺乏手机安全意识。

姚彤表示，手机用户通过下载应用、访问网站、短信链接、接听电话、扫二维码等操作，一不小心就会遭遇诈骗。“钱包丢了，只会损失部分现金，银行卡被控制了，最多是财产清零。然而手机被控制，所有的银行、理财、炒股等金融账号，都会面临巨大风险。”姚彤说。

在移动支付成为主流方式的当下，诈骗短信将“魔爪”伸向了支付与理财。据主办方介绍，2017年第一季度，360手机卫士共为全国用户拦截各类垃圾短信约24亿条，平均每天拦截垃圾短信2666万条。诈骗短信虽然仅占垃圾短信的7.6%，但其中超过七成的诈骗短信内容是冒充电商及银行，诱骗用户支付信息及相关个人隐私，以窃取用户钱财为目的。

同期，360手机卫士拦截各类钓鱼网站攻击6.2亿次，平均每天拦截691万次。其中境外彩票、虚假购物和金融证券，这三类直接威胁到用户大量资金安全的钓鱼网站占了总数的93%。(记者陶一萍、周润健)综合新华社报道



新华社发 漫画：商海春

## 直呼大名+有毒链接：诈骗短信又“升级”

诈骗短信会直呼大名？“XX，快看看这个视频”“XX，这是咱们上次聚会照片”，这类短信由于直呼网友姓名通常极具迷惑性，引诱网友点击其中附带的网址链接从而进行诈骗。

近期，360手机卫士监测到此类直呼姓名的短信呈大幅上升趋势，正以每天2万至3万条左右的数量激增，在此提示用户收到此类短信不予理会，千万不要点击其中网址链接。

近日，网友张女士就收到了一条短信，“王XX妈妈，我给你录了段视频你看看，网址XXX.XXXX.XXX”。因为学校老师经常会给家长发送孩子的视频，张女士以为是老师发来的视频，本想点开看看，突然发现短信的号码显示是青岛号码，而自己的孩子则在淮

坊读书，这才意识到可能是诈骗短信。

安全专家表示，近期此类“直呼姓名+网址链接”的诈骗短信呈明显上升趋势，网友一旦点击其中网址链接，很可能遭遇钓鱼链接，手机中被植入木马病毒，产生窃取用户隐私、偷耗手机流量、后台频繁自启、推送广告等恶意行为。更为危险的是，利用手机中的隐私信息，不法分子还可轻松盗刷网友网银、支付账户中的存款，严重威胁网友的财产安全。

360手机卫士提醒，网友收到此类短信不要轻信，更不要随意点击来源不明、安全性未知的网址；如不慎点击网址链接，其中指向的手机APP不要下载使用，不在不明界面填写自己的个人信息，尤其是密码、验证码等重要信息；及时使用手机安全管理类软件查杀手机木马。(记者周润健)据新华社天津电

## 大数据讲述

## 清理手机垃圾的“故事”

你是否有这种烦恼：再好的手机用了一段时间之后，总会变得越来越慢，越来越卡？尤其是内存较小的手机，经常会弹出“内存不足”的提示。每当此时，就说明你该清理内存垃圾了。

近日，一项针对安卓手机用户使用习惯的大数据调查表明，看似简单的垃圾清理行为，也能反映出一些有意思的现象。

1. 年轻人清理手机垃圾最勤快。调查显示，每天清理手机垃圾的群体中，48岁以下的手机用户占92%。其中，18-28岁的用户占比为44%，29-48岁的用户占比29%，17岁以下的用户占比19%。而49岁以上的用户仅占比8%。

2. 21时是清理手机垃圾最热时段。根据调查，用户每天清理手机垃圾文件最为集中的时段为21时，其次为中午12时。

3. 各地用户手机垃圾来源差异化明显。数据显示，按区域划分，北京、广东、上海、江苏、辽宁、内蒙古等地每日人均清理手机垃圾较多，但各地用户的手机垃圾来源各不相同。比如广东用户手机游戏和在线购物产生的垃圾高于其他省份，辽宁用户视频直播类应用产生的垃圾高于其他省份。

4. 不同品牌手机的垃圾文件主要来源也不同。分析发现，在各品牌手机中，华为手机用户较其他品牌更喜欢看视频和拍照；OPPO手机用户更偏爱拍照和玩游戏；而小米手机用户玩游戏产生的垃圾文件远高于其他品牌手机。

此项调查由国内手机软件开发商猎豹移动公司完成，抽选了“猎豹清理大师”2500万国内手机用户的清理行为作为样本。猎豹移动公司软件专家李铁军介绍，“猎豹清理大师”仅能获取被清理垃圾数据的大小和类型，不能获取文件的具体内容，不涉及隐私保护问题。

(记者季小波)据新华社北京电

北斗七星是指引方向的星座，在“丝绸之路”的历史上，中华北斗文化在广大沿线地区留下诸多印记，影响深远。新时代，北斗卫星导航系统是中国高科技走向世界的国家名片。如能将北斗科技和北斗文化相结合，打造成文化推广的主打产品，向全球推广，将可成为促进民心互通的纽带，为中国企业走出国门保驾护航。

# 北斗，「科技+文化」完美组合的国家名片

古代“丝绸之路”的核心意象是什么？顾名思义，丝绸。丝绸完美诠释了汉唐盛世的生活方式、审美和价值观，是对“文化自信”和“软实力”的展示。软实力的背后则是政治、经济、军事等“硬实力”的支撑。“软硬”相结合，才使丝绸之路得以世界闻名。

把目光拉回到今天，从国际视野来看，中国通过“一带一路”所能呈现的核心意象是什么呢？是古老而悠久的历史？还是当下中国直面竞争、参与挑战的崭新形象？

## 丝路“秘籍”可借鉴

丝绸、瓷器、茶道都是中国产品走向世界的成功案例。它们是中华文明集大成者，从审美、价值观、生活方式等角度，引领全球潮流。丝路的成功秘籍就是文化先行，再以产品带动文化交流，继而又用文化(审美、价值观)提升产品价值，达成良性循环。

今天，高铁、核电、北斗都是有利的国家名片，但在海外推广中，却面临着落地难等困境。这当然与我国自主技术和国际顶尖尚有一些差距，以及发达国家设置的贸易壁垒有关，但文化等“软实力”因素也不容忽视。我们有没有取得足够的文化共鸣和价值认同？有没有让沿线民众从一首歌、一本小说、一部动漫、一部电影开始，共享中国精彩故事，找到最佳的文化共通点？

自2013年，习近平总书记提出共建“丝绸之路经济带”和“21世纪海上丝绸之路”的重大倡议以来，“一带一路”沿线国家日益成为中国企业对外投资的热土。据商务部数据，2014至2016年，中国与沿线国家贸易总额超过3万亿美元，对沿线国家投资累计超过500亿美元。

“一带一路”倡议提出近4年来，中国不断与沿线国家展开产品、服务、技术、资本等层面的合作；“中国制造”“中国建设”“中国服务”也日益受沿线国家的欢迎。与之相比，中国的“文化产品名片”走出去的脚步似乎慢了一点点。

以史为镜，可知兴替。我们应当汲取“丝路”的成功经验：1. 中华优秀传统文化精华要真正走出去。2. 要培养讲“中国故事”的能力，打造体系化的主流文娱产品。3. 产业集群和创新应用代表了国家形象，应在这些领域将文化与商业相结合，精耕细作，顺势而为。

## 北斗可作“一带一路”文化推广主打产品

“北斗”这个响亮的名字具备有效结合文化、文娱产品和高科技产业的潜能，可以被打造为“一带一路”文化推广的主打产品。

北斗文化是什么？北斗是全球认知的天文星相，体现了中华民族对宇宙星空的探索。在观察星相运行规律的过程中，我们的祖先发现北斗具备指示方向、测算时间的特定功能。经过历史演变，不断赋予其丰富人文内涵，北斗文化因而逐渐形成，并从黄河流域、中原地区开始扩散，输出影响。几千年来，北斗文化向西翻过崇山峻岭，向东渡过滔天巨浪，在“一带一路”沿线地区也有大量文物、民俗可佐证。

北斗文娱产品是什么？以北斗文化为核心载体，有吸引力、可持续、高端大气上档次的体系化、主流文娱产品，让沿线民众从同一首歌、一本小说、一部动漫、一部电影开始，共享中国精彩故事。

北斗科技是什么？北斗、高铁、核电，都是中国现阶段高科技成果的代表，是国家名片。伴随大飞机、墨子号、嫦娥、天宫一号等航空航天领域一颗颗闪亮明珠滑过天际，我们应该思考：如何将这些明珠，串成中国高科技品牌的“珍珠项链”。要知道，这些航天品牌唯有形成组合拳，才是一条真正的“空中丝绸之路”，而北斗可以说是其中最醒目的标志之一。伴随北斗卫星导航系统全球组网，“星汉图腾”北斗，将再度发挥时代价值，指引全新的发展方向。

北斗文化扎根于中华五千年悠久历史，完美结合国之重器——北斗卫星导航系统，有五个特点：1. 体现国家战略，结合时代主流，探索星空；2. 全球通行，在悠久历史中传承有序，全世界影响广泛；3. 有神秘感：北斗隐迹，示而不语，符合国际主流审美品位；4. 内涵丰富，形象正面，有极强代表性；5. 符号化标志，便于识别，易于传播。

总而言之，北斗文化不单能提升行业品牌，促进产业结合，帮助国家技术装备走出去。更为难得的是，这个核心意象产生的过程极具启示意义，在传播北斗文化的过程中，将引导年轻一代从古老中华文明中汲取营养，传承优秀传统文化。

(汪柯)