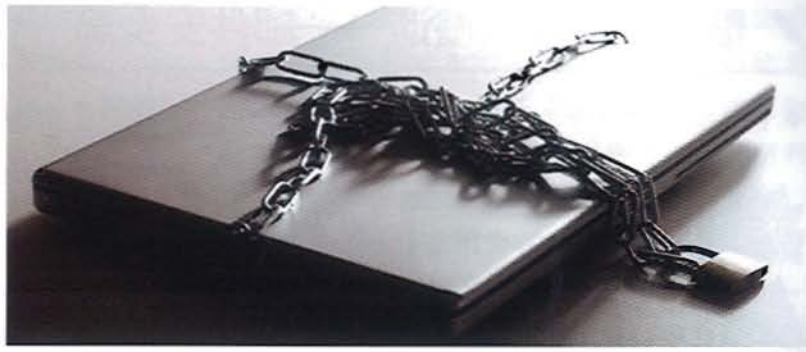
信息安全小百科

计算机病毒与信息安全

2017年5月12日，一款名为Wannacry的勒索蠕虫病毒肆虐全球，全球150个国家和地区的约30万台电脑遭到攻击，影响巨大。



计算机感染病毒的常见症状

在信息化和网络化时代，个人计算机已不再是信息孤岛，只要与外界进行数据交换，就有感染病毒的可能。打个比方，无论我们多么注重保养身体，也不能避免生病，生病了需要就医，医生会根据症状判断得了什么病，然后对症治疗。同样，计算机也会生病，即中毒，那么就需要先了解计算机生病的症状，判断计算机是否“中毒”，进而给计算机进行杀毒治疗。那么，计算机“中毒”后有哪些常见症状呢？

1.打开浏览器后出现的页面不是以往默认的页面，主页地址可能变成了陌生网址，且很难修改到默认的页面。

2.计算机桌面背景多出类似“在线小游戏”“免费电影”“网上淘宝”“软件下载”“无名软件”等广告图标，双击打开后，内容往往是网络商品推介等。

3.如果网络状况正常，但联网游戏时却经常掉线，且没有特别提醒，这很可能是有人在暗中捣鬼，试图窃取你的账号和密码。

4.鼠标自己会移动，摄像头会自动打开，硬盘灯无故闪烁，光驱无故弹出，这很有可能表明有人在远程控制你的计算机。

5.计算机里的安全防护软件不起作用，无论是单击快捷方式还是直接运行程序均不能启动，甚至无法访问安全软件厂商的官网。

6.计算机突然运行变慢，上网也不顺畅，任务管理器中增加了许多陌生进程，且无法停止。

计算机感染病毒的防治措施

计算机病毒具有独特的复制能力，能够快速蔓延，又常常难以根除。它们能够把自身附着在各种类型的文件上，当文件被复制或从一个用户传送到另一个用户时，就随同文件一起蔓延开来。

计算机感染病毒时往往出现两种情况，可通过如下方法进行病毒查杀。

情况一：计算机可以正常运行

1.如果中毒后计算机可以正常运行，那么千万不要再登录账号或进行修改密码等操作，应及时使用计算机杀毒软件进行病毒查杀。

2.病毒查杀完成后，一定要重启计算机，因为大多数病毒都是在重启后，才会被彻底清除。重启完成后，应修改中毒期间使用过的账号和密码。

情况二：计算机无法正常运行

1.如果中毒后计算机无法正常运行，如出现程序打不开，计算机键盘、鼠标被锁定等情况，一定要及时拔掉网线或直接关闭路由器。

2.在重启计算机的过程中连续按F8，进入网络安全模式，随后正常连接网络，下载计算机杀毒软件，即可进行病毒查杀。

另外，在查杀病毒时，为确保病毒被彻底清理，一定要选择正规的计算机杀毒软件，还要养成定期查杀病毒的习惯。END

（康双勇/国家保密科技测评中心）

（栏目编辑：郝君婷）

要 闻

公安部正制定网络安全条例　大数据保护机制将完善

公安部网络安全保卫局副局长在日前闭幕的2017中国国际大数据产业博览会上透露，目前公安部正在制定网络安全保护条例，拟将大数据、云平台、物联网、工业控制系统纳入其中，并进一步完善等级保护措施，重点加强对国家关键基础设施和大数据的安全保护。据介绍，条例拟将大数据保护等级定为第三级以上，在大数据安全保护措施方面：一是开展摸底调查，全面掌握大数据安全保护状态；二是针对数据采集、存储、处理、应用、销毁等，提出不同的安全保护等级制度。另据悉，公安部已组织相关单位制定网络安全等级保护技术标准中的大数据扩展要求，拟于2017年正式发布实施。

（http://www.bigdata-expo.org）

香格里拉对话会　聚焦亚太安全威胁

2017年6月2~4日，第16届香格里拉对话会在新加坡举行。新技术的产生发展使非传统安全领域，特别是网络攻击成为亚太国家在本次对话会上的讨论焦点。针对如何应对新技术发展对非传统安全带来的冲击，与会人员分析认为：军事大国和技术强国应体现责任担当，加强信息交流与分享，评估黑客攻击等在物联网领域扩散带来的安全挑战，同时将新技术优势用于灾难预警、国际反恐、打击跨国犯罪和人道主义救助等领域。

（http://www.it.people.com.cn）

两项两化融合管理体系国家标准发布

2017年6月7日，GB/T 23000-2017《信息化和工业化融合管理体系基础和术语》和GB/T 23001-2017《信息化和工业化融合管理体系要求》两项两化融合管理体系国家标准正式发布。这两项国家标准的发布是两化融合管理体系标准研制的重要里程碑，标志着两化融合管理体系贯标工作进入了新阶段。下一步将加快这两项国家标准等两化融合管理体系标准的全面普及，一是做好顶层设计和总体规划；二是深入开展试点示范；三是持续建设数据地图，持续推进企业两化融合自评估、自诊断和自对标；四是健全市场化运行体系，完善贯标工作的全流程服务体系，建立开放透明的监督管理机制，扩大两化融合管理体系评定结果的社会采信范围。

（http://www.cnii.com.cn）

数 字

90%

360最新发布的《2017年第一季度中国手机安全状况报告》显示，正常网站被黑之后用来钓鱼的占比9.1%，其余90.9%的钓鱼网站由不法分子自建。

5000

《中华人民共和国网络安全法》6月1日起实施，规定贩卖50条个人信息可入罪，提供个人信息违法所得5000元以上可入刑。

2.5亿

全球知名安全公司Check Point近日发现一款恶意软件Fireball已感染2.5亿台电脑，该软件允许黑客操控受害者浏览器、更改搜索引擎并窃取用户私人数据。

技 术

海洋国家实验室争夺E级超算“皇冠”

青岛海洋科学与技术国家实验室（以下简称海洋国家实验室）作为我国海洋领域首个获批组建的国家实验室，坚持以国家战略任务为导向，按照抢占海洋科技创新制高点，服务国家重大海洋战略的总体要求，自2015年10月正式启用以来，一直积极推进E级超算工作。

E级超算作为“国之利器”，对于支撑海洋国家实验室抢占全球海洋科研制高点、高效服务于国家海洋战略，保障海洋国防安全、海洋经济和生态安全等方面均具有重要战略和现实意义。专家呼吁尽快启动海洋国家实验室E级超算中心建设。

（http://www.cac.gov.cn）

北斗地基增强系统一期建设完成

近日，北斗地基增强系统一期通过验收。专家组评审认为，我国已基本建成自主可控、全国产化的北斗地基增强系统，初步形成基于北斗的一体化高精度应用服务体系，系统建设迈入边建、边用、边运行、边服务的新阶段。

该系统是北斗系统服务体系的重要组成部分。建成以北斗为主兼容其他系统的高精度位置服务网络，将为确保国家高精度时空信息安全提供根本保障。系统建设坚持国家主导、军民融合，同时充分发挥市场作用，搭建北斗高精度位置服务运营平台，开展增值服务商业运营，已形成系列高精度服务产品并面向市场提供服务。

（http://www.xinhuanet.com/）

中国首台微波光子雷达诞生 分辨率惊人

中科院电子学研究所网站6月12日报道，该所成功研制出中国第一台微波光子雷达样机，并通过外场非合作目标成像测试，获得国内第一幅微波光子雷达成像图样，在图像分辨率上比国际水平高出一个数量级。

微波光子雷达，以光子为信息载体，利用丰富的光谱资源和灵活的光子技术，能够更好、更快地产生和处理雷达宽带信号，具有快速成像、高分辨率和清晰辨识目标的能力。微波光子雷达对目标精细结构和特征的快速识别，使其不仅能够应用于作战平台对小型化目标的实时辨识，也能为无人智能设备提供准确的环境信息，在军民两栖领域具有重要意义。

（http://www.sohu.com）

数 字

6亿

近日，工信部发布的《2017年1~4月电子信息制造业运行情况》显示，2017年1~4月份我国生产手机超6亿部，增长9.8%。

125亿

据IDC预测，2017年全球认知计算和人工智能（AI）收入规模将达到125亿美元，美国是目前认知计算和人工智能支出最大的市场。

300亿

IBM近日宣布，将推出全球首个5纳米工艺芯片，可将300亿个5纳米开关电路集成在指甲盖大小的芯片上，预计于2020年开始规模量产。

美国防部数据被承包商泄露公开至亚马逊服务器

网络安全公司UpGuard近日发现，来自美国国家地理空间情报局（NGA）的某美国军方项目，将超过6万份敏感文件存储于Amazon云存储服务器，且无需任何身份验证即可访问。

根据报道，这些文件由美国规模最大的国防情报承包商之一的博思艾伦咨询公司（Booz Allen Hamilton）存储于某台公开的Amazon服务器上，其中包含大量与美国政府系统相关的密码，更严重的是，这批泄露的文件中包含的数据甚至涉及本应受到高度保护的五角大楼系统管理访问权限的主凭证。

尽管这些文件已无法继续通过网络访问，但可能已有人完成下载，这意味着美国情报机构将因此遭受极为严重的潜在影响。

（https://www.easyaq.com）

Hadoop服务器人为配置不当 或致全球数据泄露达5120TB

HackerNews6月4日消息，网络犯罪分子近期开始针对配置不当的Hadoop Clusters 与 CouchDB服务器展开攻击活动。目前，全球因Hadoop分布式文件系统（HDFS）配置不当导致的数据泄露或达5120TB。

据搜索引擎Shodan分析显示，全球将近4500台设备因使用Hadoop分布式文件系统（HDFS）时配置不当，致使服务器出现数据泄露现象，这些服务器主要位于美国（1900）、中国（1426）、德国（129）与韩国（115）等。调查显示已暴露的HDFS多数托管于云端，其中涉及亚马逊1059个服务器、阿里云507个服务器。

安全专家建议企业设备管理人员在安全模式下，按照指令说明正确配置Hadoop服务器。

（http://www.cert.org.cn）

政府部门和金融行业已成网络攻击的最大目标

最新研究表明，2016年针对全球政府部门的网络攻击与2015年相比翻了一番，从所有网络安全攻击的7%上升到14%。针对金融部门的网络攻击也从2015年的3%大幅上升到2016年的14%。制造业以13%的份额排在第三位，而在2015年行业网络安全攻击名单高居榜首的零售行业则下降到第四位（11%）。

这些数据来自于Dimension Data公司的“NTT Security 2017全球威胁情报报告”的执行指南，这个指南是从NTT安全公司及其他NTT的运营公司（包括Dimension Data）收集的数据汇总，来自五大洲10000个客户端的网络，3.5万亿个安全日志，62亿次袭击企图。

（http://www.secdoctor.com）

（本栏目数据内容摘自相关媒体、网站）

1000亿

6月6日，中央网信办、财政部共同发起设立中国互联网投资基金，总规模1000亿元，其中首期规划募集300亿元已全部认缴到位。

5万亿

日本三大移动通信运营商从2010年开始为用户提供5G服务，对于5G移动通信网络建设的投资总额将达到5万亿日元。

8万亿

据安全网络公司Juniper最新预估，网络犯罪经济成本将于2022年飙升至8万亿美元，预计将有5亿的客户数据记录被盗取。

（栏目编辑：郝君婷）