网络信息安全周报

【2017】第 12 期

党委宣传部
信息网络中心　编

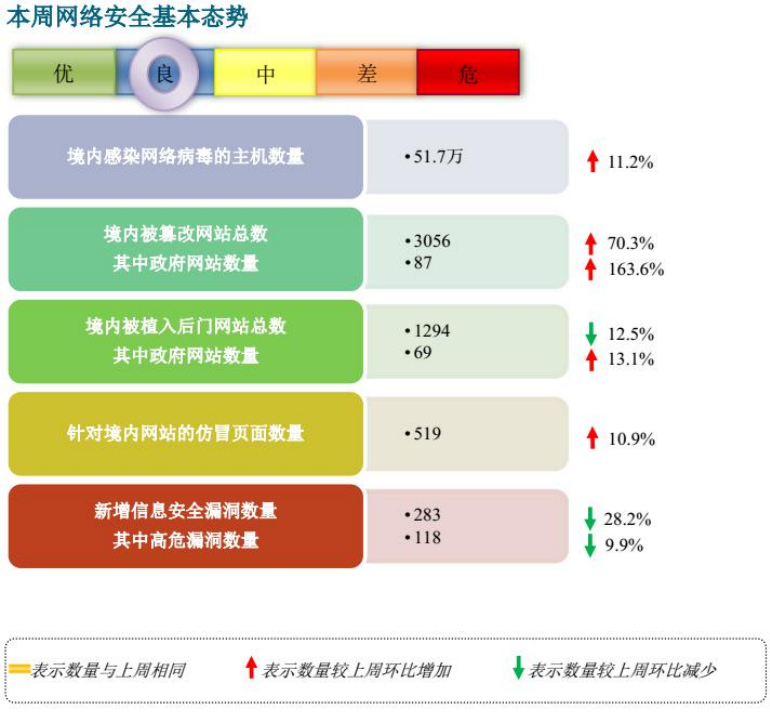
2017 年 5 月 18 日

本期要目

- 权威发布：全国网络安全信息与动态（2017 年 5 月 1 日—5 月 7 日）
- 城院 IT 综合业务管理平台统计信息（2017 年 5 月 2 日—5 月 9 日）
- 关于防范 Windows 操作系统勒索软件 Wannacry 的情况通报
- 普通用户如何应对恶性勒索病毒?

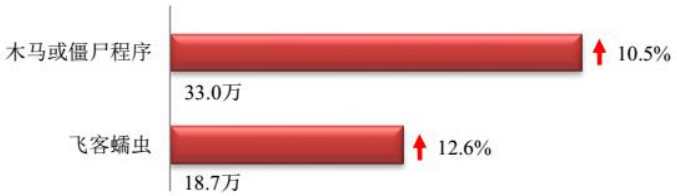
网络安全信息与动态（2017 年 5 月 1 日—5 月 7 日）

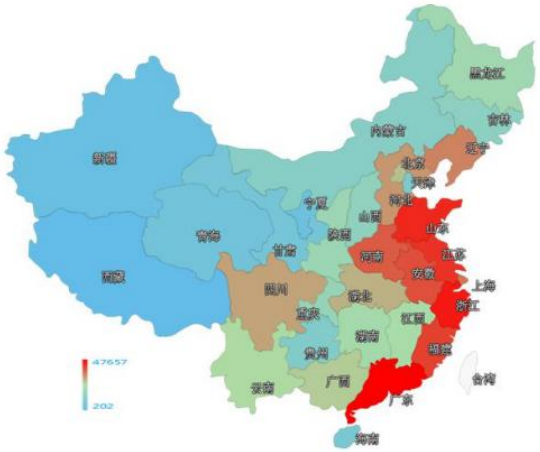
根据国家互联网应急中心最新公告数据：



本周网络病毒活动情况

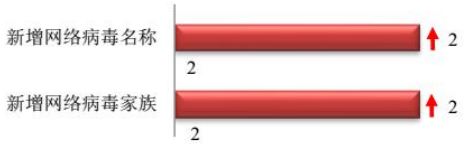
本周境内感染网络病毒的主机数量约为 51.7 万个，其中包括境内被木马或被僵尸程序控制的主机约 33.0 万以及境内感染飞客（conficker）蠕虫的主机约 18.7 万。





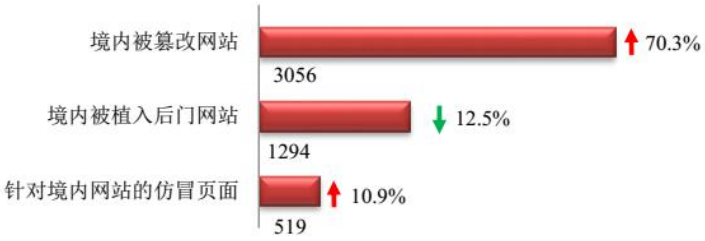
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、浙江省和山东省。

本周 CNCERT 捕获的新增网络病毒文件，按网络病毒名称统计新增 2 个，按网络病毒家族统计新增 2 个。



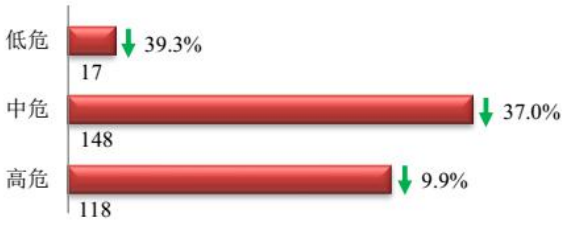
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 3056 个；境内被植入后门的网站数量为 1294 个；针对境内网站的仿冒页面数量为 519。



本周重要漏洞情况

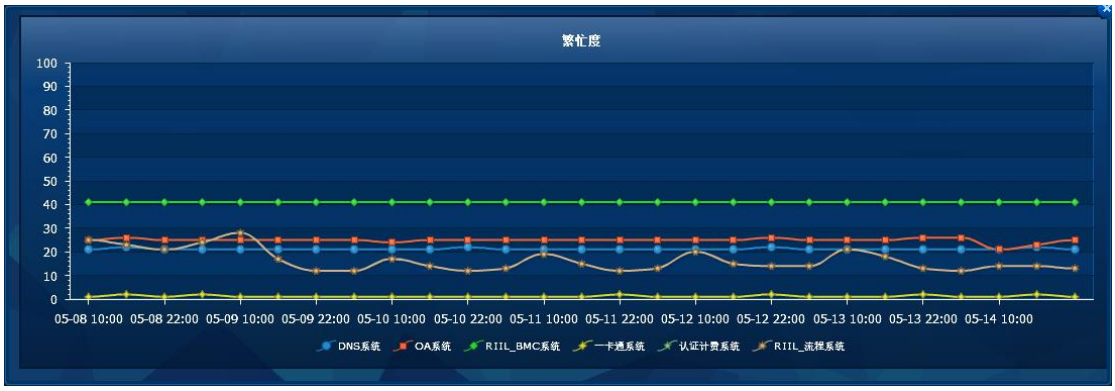
本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 283 个，信息安全漏洞威胁整体评价级别为中。



城院 IT 综合业务管理平台统计信息

（2017 年 5 月 8 日—5 月 15 日）

主要业务服务繁忙度



网站集群网页更新情况统计

站点名称	合计	站点名称	合计
兰州城市学院	18	传媒学院	0
文史学院	11	城市信息与系统科学研究所	0
兰州城市学院教育评估中心	7	审计	0
教务处	7	甘肃张芝书法院	0
商学院	4	音乐学院	0
马克思主义学院	4	就业服务网	0
信息网络中心	4	美术与设计学院	0
电子与信息工程学院	4	保卫处	0
幼儿师范学院	3	路易艾黎研究中心	0
兰州城市学院校医院	3	党委宣传部	0
教育学院	3	发展规划处	0
外国语学院	3	人事处	0
化学与环境工程学院	2	电子信息科学与技术研究所	0
科学研究处	2	基本建设处	0
数学学院	2	国有资产管理处	0
体育学院	2	党委（校长）办公室	0
膳食处	2	创新创业学院	0
卡务中心	1	传媒学院（新）	0
实训中心	1	党委学生工作部	0
石油工程学院	1	甘肃文化翻译中心	0
信息技术教育与应用研究所	0	城市社会心理研究中心	0
机械工程学院	0	后勤管理处	0
职业技能鉴定所	0	档案馆	0
地理与城乡规划学院	0	党委组织部	0
心理咨询中心	0	旅游学院	0
学位办公室	0	教师发展中心	0
招生网	0	团委	0
机关党委	0	廉政网	0

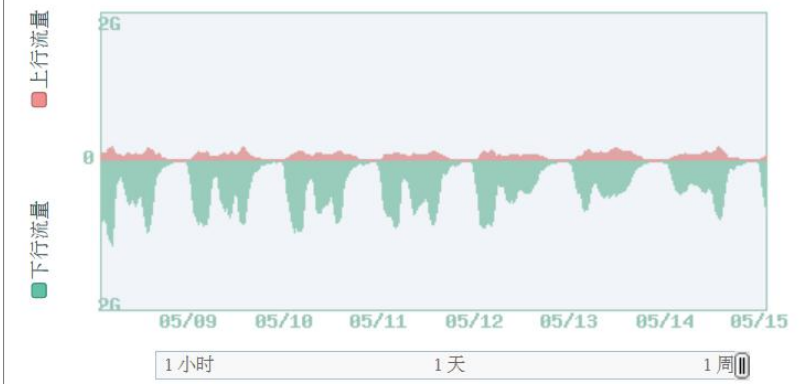
网络出口带宽情况统计

联通出口 – 1 周

接口: Agg_unicom

电信出口 – 1 周

接口: Agg_chinanet



教育网出口 – 1 周

接口: port13

关于防范 Windows 操作系统勒索软件 Wannacry 的情况通报

2017 年 05 月 13 日　来源：国家互联网应急中心

北京时间 5 月 12 日，互联网上出现针对 Windows 操作系统的勒索软件（Wannacry）攻击案例。勒索软件利用此前披露的 Windows SMB 服务漏洞（对应微软漏洞公告：MS17-010）攻击手段，向终端用户进行渗透传播，并向用户勒索比特币或其他价值物。包括高校、能源等重要信息系统在内的多个国内用户受到攻击，已对我国互联网络构成较为严重的安全威胁。

一、勒索软件情况

综合 CNCERT 和国内网络安全企业（奇虎 360 公司、安天公司等）已获知的样本情况和分析结果，该勒索软件在传播时基于 445 端口并利用 SMB 服务漏洞（MS17-010），总体可以判断是由于此前“Shadow Brokers”披露漏洞攻击工具而导致的后续黑产攻击威胁。4 月 16 日，CNCERT 主办的 CNVD 发布《关于加强防范 Windows 操作系统和相关软件漏洞攻击风险的情况公告》，对影子纪经人“Shadow Brokers”披露的多款涉及 Windows 操作系统 SMB 服务的漏洞攻击工具情况进行了通报（相关工具列表如下），并对有可能产生的大规模攻击进行了预警：

表 有可能通过 445 端口发起攻击的漏洞攻击工具

工具名称	主要用途
ETERNALROMANCE	SMB 和 NBT 漏洞，对应 MS17-010 漏洞，针对 139 和 445 端口发起攻击，影响范围:Windows XP, 2003, Vista, 7, Windows 8, 2008, 2008 R2
EMERALDTHREAD	SMB 和 NETBIOS 漏洞，对应 MS10-061 漏洞，针对 139 和 445 端口，影响范围：Windows XP、Windows 2003
EDUCATEDSCHOLAR	SMB 服务漏洞，对应 MS09-050 漏洞，针对 445 端口
ERRATICGOPHER	SMBv1 服务漏洞，针对 445 端口，影响范围：Windows XP、Windows server 2003，不影响 windows Vista 及之后的操作系统
ETERNALBLUE	SMBv1、SMBv2 漏洞，对应 MS17-010，针对 445 端口,影响范围：较广，从 WindowsXP 到 Windows 2012
ETERNALSYNERGY	SMBv3 漏洞，对应 MS17-010，针对 445 端口，影响范围：Windows8、Server2012
ETERNALCHAMPION	SMB v2 漏洞，针对 445 端口

当用户主机系统被该勒索软件入侵后，弹出如下勒索对话框，提示勒索目的并向用户索要比特币。而对于用户主机上的重要文件，如：照片、图片、文档、压缩包、音频、视频、可执行程序等几乎所有类型的文件，都被加密的文件后缀名被统一修改为“.WNCRY”。目前，安全业界暂未能有效破除该勒索软的恶意

加密行为，用户主机一旦被勒索软件渗透，只能通过重装操作系统的方式来解除勒索行为，但用户重要数据文件不能直接恢复。

图 勒索软件界面图（来源：安天公司）

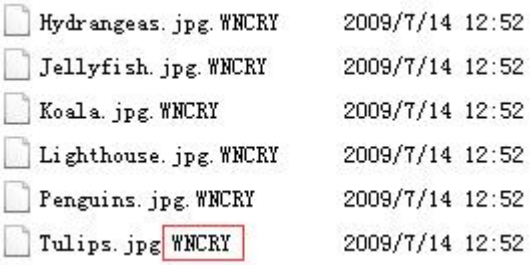


图 用户文件被加密（来源：安天公司）

二、应急处置措施

CNCERT 已经着手对勒索软件及相关网络攻击活动进行监测，5 月 13 日 9 时 30 分至 12 时，境内境外约 101.1 万个 IP 地址遭受“永恒之蓝”SMB 漏洞攻击工具的攻击尝试，发起攻击尝试的 IP 地址（包括进行攻击尝试的主机地址以及可能已经感染蠕虫的主机地址）数量 9300 余个。建议广大用户及时更新 Windows 已发布的安全补丁更新，同时在网络边界、内部网络区域、主机资产、数据备份方面做好如下工作：

（一）关闭 445 等端口(其他关联端口如: 135、137、139)的外部网络访问权限，在服务器上关闭不必要的上述服务端口(具体操作请见参考链接)；

（二）加强对 445 等端口（其他关联端口如: 135、137、139)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；

（三）及时更新操作系统补丁。

（四）安装并及时更新杀毒软件。

（五）不要轻易打开来源不明的电子邮件。

（六）定期在不同的存储介质上备份信息系统业务和个人数据。

CNCERT 后续将密切监测和关注该勒索软件的攻击情况，同时联合安全业界对有可能出现的新的攻击传播手段、恶意样本进行跟踪防范。

附：参考链接：

http://thehackernews.com/2017/04/window-zero-day-patch.html?m=1&from=groupmessage

微软发布的官方安全公告：

https://blogs.technet.microsoft.com/msrc/2017/04/14/protecting-customers-and-evaluating-risk/?from=timeline&isappinstalled=0

CNVD 安全公告：

http://www.cnvd.org.cn/webinfo/show/4110

安天防护手册：

http://www.antiy.com/response/Antiy_Wannacry_Protection_Manual/Antiy_Wannacry_Protection_Manual.html

普通用户如何应对恶性勒索病毒?

❷

本次病毒利用 Windows 漏洞自动攻击

依次点击来**开启 Windows 系统防火墙**

▼

按照控制面板

▼

网络和 Internet

▼

网络和共享中心

▼

更改适配器设置

▼

网络属性

▼

取消勾选

Microsoft 网络文件和打印机共享

▼

重启电脑

❸

有很多朋友不喜欢给电脑打补丁，
这其实是很不好的习惯。
为了更好地抵御病毒，
大家可下载 Windows 系统补丁 3.14 并安装。

立即下载
Windows 3.14 系统补丁

❹

大家千万不要点击不明邮件内的链接信息以及
来源不明的文件，避免“引火上身”。

一旦您的电脑被感染，请立即断网，
防止病毒进一步扩散到局域网内的其他电脑。

抄送：校领导