

网络安全信息与动态周报

本周网络安全基本态势



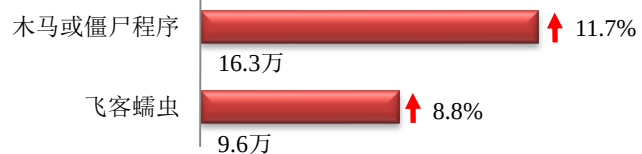
表示数量与上周相同

↑ 表示数量较上周环比增加

↓ 表示数量较上周环比减少

本周网络病毒活动情况

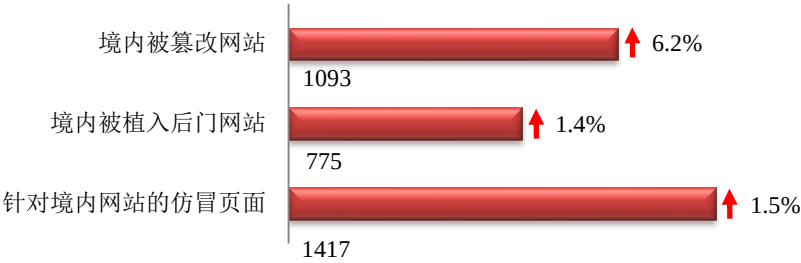
本周境内感染网络病毒的主机数量约为 25.9 万个，其中包括境内被木马或被僵尸程序控制的主机约 16.3 万以及境内感染飞客（conficker）蠕虫的主机约 9.6 万。





本周网站安全情况

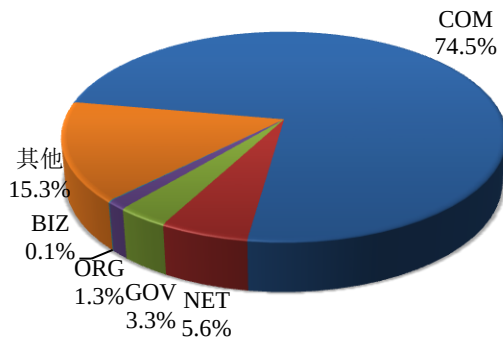
本周 CNCERT 监测发现境内被篡改网站数量为 1093 个；境内被植入后门的网站数量为 775 个；针对境内网站的仿冒页面数量为 1417。



本周境内被篡改政府网站（GOV 类）数量为 36 个（约占境内 3.3%），与上周持平；境内被植入后门的政府网站（GOV 类）数量为 11 个（约占境内 1.4%），较上周环比下降了 31.3%；针对境内网站的仿冒页面涉及域名 515 个，IP 地址 201 个，平均每个 IP 地址承载了约 7 个仿冒页面。

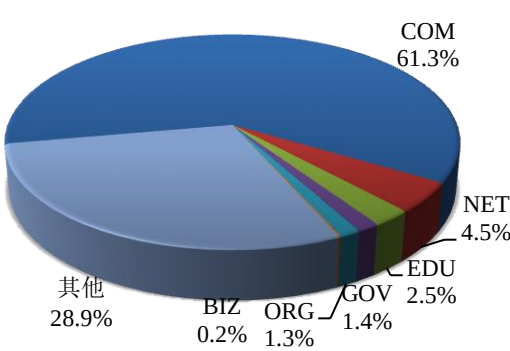
本周我国境内被篡改网站按类型分布
(7/23-7/29)

CNCERT/CC



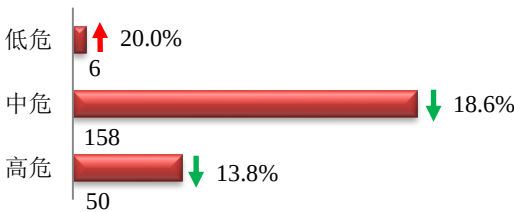
本周我国境内被植入后门网站按类型分布
(7/23-7/29)

CNCERT/CC

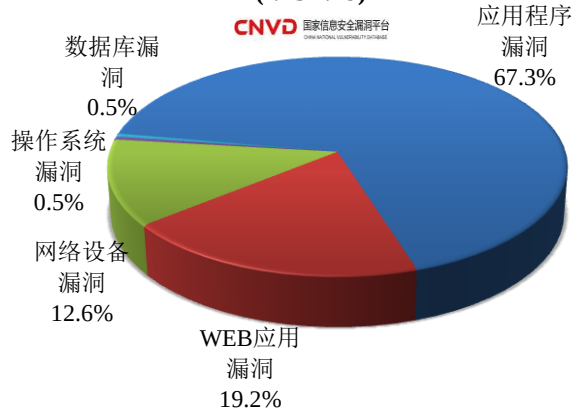


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 214 个，信息安全漏洞威胁整体评价级别为中。



本周CNVD收录漏洞按影响对象类型分布
(7/23-7/29)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是 WEB 应用漏洞和网络设备漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

CNVD漏洞周报发布地址

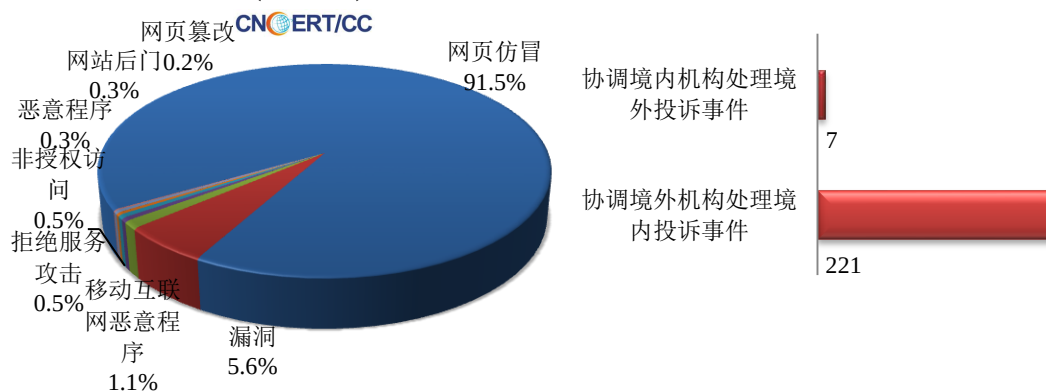
<http://www.cnvd.org.cn/webinfo/list?type=4>

国家信息安全漏洞共享平台(缩写CNVD)是CNCERT联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

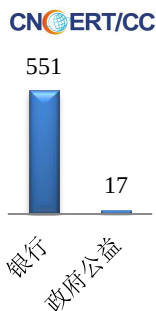
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 621 起，其中跨境网络安全事件 228 起。

本周CNCERT处理的事件数量按类型分布
(7/23-7/29)



本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 568 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 551 起和政府公益仿冒事件 17 起。

本周CNCERT处理网页仿冒事件数量
按仿冒对象涉及行业统计(7/23-7/29)

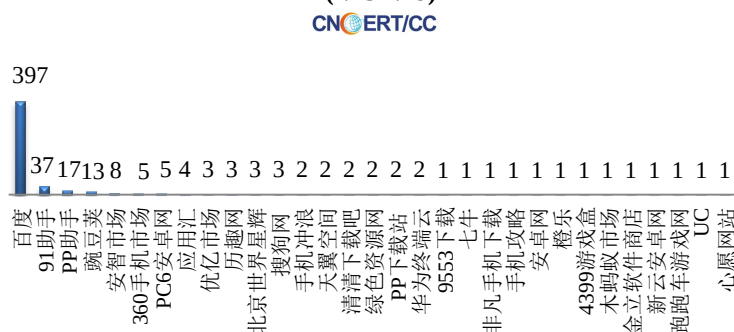


本周CNCERT协调境内域名注册机构处理网
页仿冒事件数量排名(7/23-7/29)



本周，CNCERT 协调 31 个应用商店及挂载恶意程序的域名开展移动互联网恶意代码处理工作，共处理传播移动互联网恶意代码的恶意 URL 链接 523 个。

本周CNCERT协调手机应用商店处理移动互联网恶意
代码事件数量排名
(7/23-7/29)



业界新闻速递

1、美军专设工作组应对俄网络攻击 普京称俄未干涉美内政

参考消息网 7 月 24 日消息 俄新社 7 月 23 日报道称，美国网络司令部司令保罗·中曾根表示，该司令部成立了专门工作组以应对俄罗斯在网络空间采取的行动。保罗·中曾根在科罗拉多州阿斯彭举行的安全论坛上表示：“我们成立了一个俄罗斯小组，就像美国情报机构联合会 2016 至 2017 年做的那样。”他还称：“俄罗斯拥有强大的网络能力，我们将要与其对抗。如果对抗发生，毫无疑问我们能够战胜他们。”美国决定加强对网络空间的保护发生在其指控俄罗斯干涉美国 2016 年总统选举和企图干涉今年国会选举的背景下。普京在赫尔辛基会见特朗普后表示，俄罗斯未曾也无意干涉美国内政。他还建议美国组建网络安全工作组讨论他们担心的问题。

2、共分 5 个等级 日本政府敲定今后 3 年的网络安全战略

环球网 7 月 25 日消息 距离 2020 年东京奥运会和残奥会只剩下 2 年时间。在此背景下，日本政府敲定了今后 3 年的“网络安全战略”，决定在网络安全方面采用新标准，把针对水电等重要基础设施的网络攻击分成 5 个级别进行评估和公布，以便妥善采取应对措施。据日本 NHK 电视台 7 月 25 日报道，“网络安全战略”提出，在物联网技术不断发展的背景下，网络攻击对稳定安全的日本国民生活造成威胁，甚至出现个别国家参与网络攻击的事例。鉴于此，日本政府将采用新的网络攻击评估和公布标准，把针对水电、机场等重要基础设施的网络攻击按照严重程度分成 0 到 4 共 5 个级别，以便于各相关部门等准确掌握事态的严重程度，妥善采取应对措施。“网络安全战略”提出，将设置“网络安全应对调整中心”，统一进行相关信息的收集管理。另外，日本政府将携手相关企业等，官民共享国内外网络攻击方面的信息，推进“积极的网络防御”措施，防患于未然。此外，日本政府还将在虚拟货币、汽车自动驾驶等高新技术方面加强网络攻击的防范措施。

3、欧盟发布保护云数据个人隐私技术成果

科技部网站 7 月 23 日消息 欧盟近期发布了一项与云数据个人隐私保护有关的最新科研成果，该成果由欧盟“地平线 2020”计划资助下的“云安”(SafeCloud)项目组完成。欧盟高度重视个人隐私数据保护，5 月 25 日生效的《通用数据保护条例》为个人隐私保护提供了有力的法律保障，而近期“云安”项目公布的个人隐私数据保护技术为个人隐私保护提供了可选择的技术支持。“云安”项目所采用的技术架构中采用了两项起着核心作用的技术——分区和纠缠，项目组在整个数据管理堆栈中使用这两项技术，既保证了通讯安全，又保证了个人数据得以妥善存储。“云安”技术充分授权用户保护个人数据的安全，让用户掌控存储个人资料的域，并让其选择纠缠的级别，通过这种方式让用户既能利用云数据、又能够保护其个人隐私；既能保证了云数据的运算性能，又保证了云数据的扩展性。“云安”项目由葡萄牙、瑞士、德国和爱沙尼亚等国的科研机构联合承担，执行期自 2015 年 9 月至 2018 年 8 月。

4、智利 1.4 万信用卡资料被黑客组织盗取

环球网 7 月 26 日消息 据新加坡《联合早报》26 日报道，智利政府周三(25 日)晚透露，黑客盗取了智利约 1.4 万张信用卡的资料，并将这些资料公布在社交媒体上。报道称，在这起案件中，黑客公布了信用卡卡号、有效期限及安全码，受攻击影响的银行包括桑坦德银行(Santander)、伊塔乌银行(Itau)、丰业银行(Scotiabank)和智利银行(Banco de Chile)，这些银行已通知客户遭入侵一事。报道称，智利政府并未透露此次信用卡资料被盗事件可能造成的损失。智利政府的银行监管机构表示，这起袭击行动是黑客组织“影子经纪人”(Shadow Brokers)展开的，该组织因入侵美国国家安全局(NSA)而闻名。今年 6 月，智利银行曾透露，黑客盗取了该银行 1000 万美元(约 1360 万新元)。智利银行当时说，黑客是从东欧或亚洲发动袭击，部分遭盗窃的款项最后被汇到香港。

5、推特清理逾 14.3 万款应用 防止剑桥分析式丑闻

凤凰网 7 月 25 日消息 据《财富》北京时间 7 月 25 日报道，Twitter 当地时间星期二表示，它在 2018 年 4-6 月期间对恶意应用进行了清理，共下架逾 14.3 万款应用。Twitter 曾在一篇博文中称，它“不容忍利用我们的

API(应用编程接口)制造垃圾信息、操控会话、借助 Twitter 侵犯人们的隐私”。Twitter 清理恶意应用正值 Facebook 的剑桥分析数据泄露丑闻发酵之际。Facebook 面临国会议员的激烈批评：没有能阻止一名学术研究人员通过在其平台上开发的一款应用窃取大量用户信息。与 Facebook 和谷歌旗下 YouTube 一样，Twitter 也因没有能阻止俄罗斯相关部门在其服务上创建账户，在美国大选期间传播虚假信息受到密切关注。

关于国家互联网应急中心（CNCERT）

国家互联网应急中心是国家计算机网络应急技术处理协调中心的简称（英文简称为 CNCERT 或 CNCERT/CC），成立于 2002 年 9 月，是一个非政府非盈利的网络安全技术协调组织，主要任务是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展中国互联网上网络安全事件的预防、发现、预警和协调处置等工作，以维护中国公共互联网环境的安全、保障基础信息网络和网上重要信息系统的安全运行。目前，CNCERT 在我国大陆 31 个省、自治区、直辖市设有分中心。

同时，CNCERT 积极开展国际合作，是中国处理网络安全事件的对外窗口。CNCERT 是国际著名网络安全合作组织 FIRST 正式成员，也是 APCERT 的发起人之一，致力于构建跨境网络安全事件的快速响应和协调处置机制。截至 2017 年，CNCERT 与 72 个国家和地区的 211 个组织建立了“CNCERT 国际合作伙伴”关系。

联系我们

如果您对 CNCERT《网络安全信息与动态周报》有何意见或建议，欢迎与我们的编辑交流。

本期编辑：韩志辉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158