国家互联网应急中心

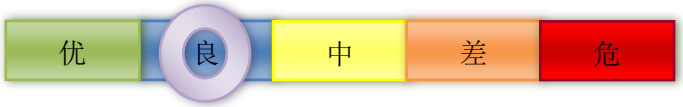
网络安全信息与动态周报

2018 年第 29 期

7 月 16 日-7 月 22 日

CNCERT/CC

本周网络安全基本态势

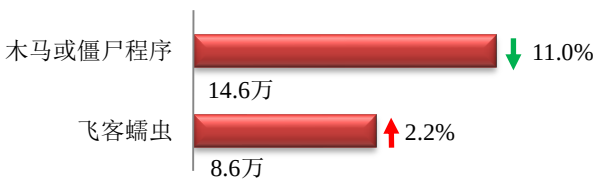


境内感染网络病毒的主机数量	• 23.4万	6.4%
境内被篡改网站总数 其中政府网站数量	• 1029 • 36	3.3% 33.3%
境内被植入后门网站总数 其中政府网站数量	• 764 • 16	3.9% 33.3%
针对境内网站的仿冒页面数量	• 1396	20.6%
新增信息安全漏洞数量 其中高危漏洞数量	• 257 • 58	= 23.7%

=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

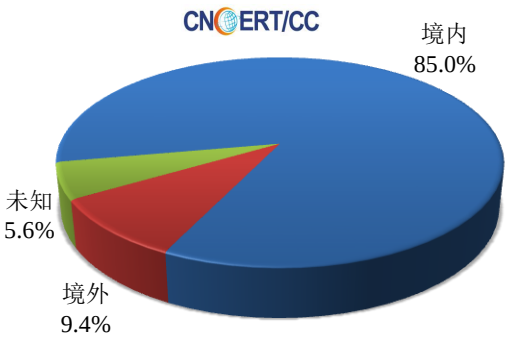
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 23.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 14.6 万以及境内感染飞客（conficker）蠕虫的主机约 8.8 万。

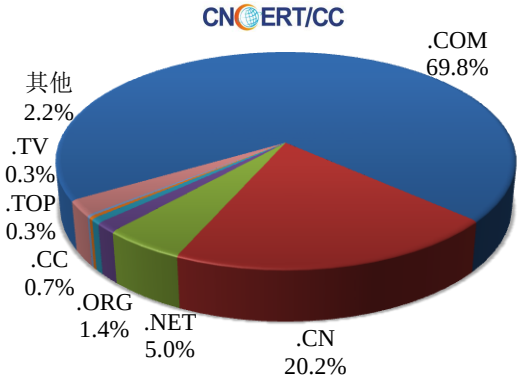


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 3858 个，涉及 IP 地址 23794 个。在 3858 个域名中，有 9.4%为境外注册，且顶级域为.com 的约占 69.8%；在 23794 个 IP 中，有约 51.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 195 个 IP。

本周放马站点域名注册所属境内外分布
(7/16-7/22)



本周放马站点域名所属顶级域的分布
(7/16-7/22)



针对 CNCERT 自主监测发现以及各单位报送数据，CNCERT 积极协调域名注册机构等进行处理，同时通过 ANVA 在其官方网站上发布恶意地址黑名单。

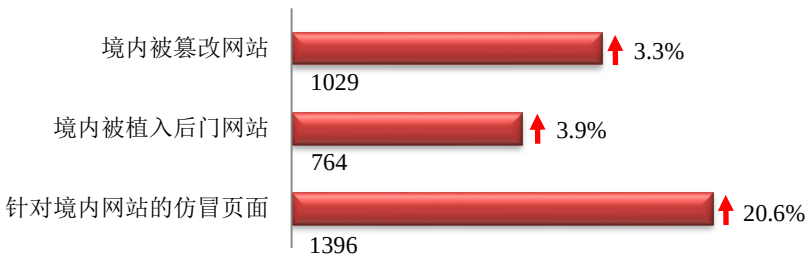
ANVA恶意地址黑名单发布地址

http://www.anva.org.cn/virusAddress/listBlack

中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由中国互联网协会网络与信息安全工作委员会发起、CNCERT 具体组织运作的行业联盟。

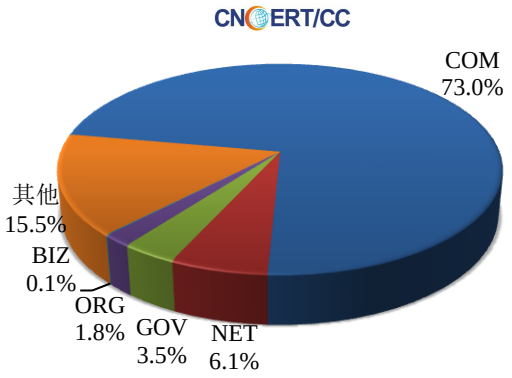
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1029 个；境内被植入后门的网站数量为 764 个；针对境内网站的仿冒页面数量为 1396。

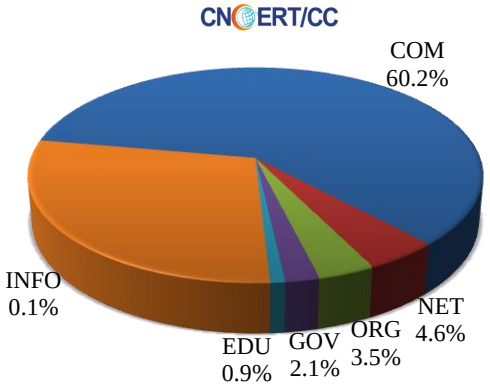


本周境内被篡改政府网站（GOV 类）数量为 36 个（约占境内 3.5%），较上周环比上升了 33.3%；境内被植入后门的政府网站（GOV 类）数量为 16 个（约占境内 2.1%），较上周环比上升了 33.3%；针对境内网站的仿冒页面涉及域名 460 个，IP 地址 225 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(7/16-7/22)

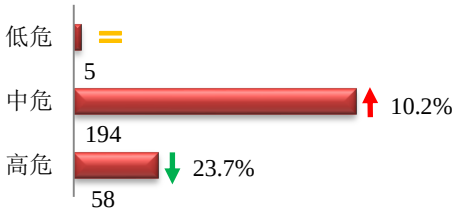


本周我国境内被植入后门网站按类型分布
(7/16-7/22)

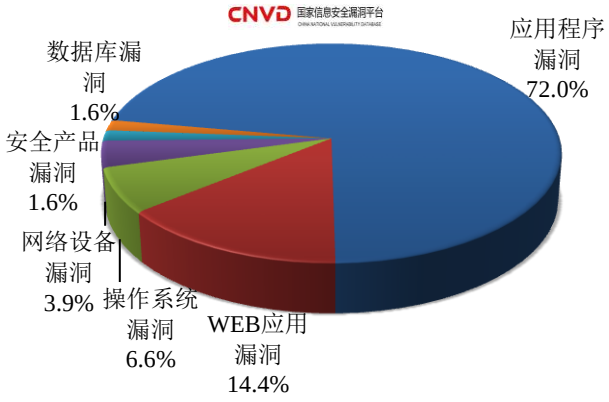


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 257 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
(7/16-7/22)



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 应用漏洞和操作系统漏洞。

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

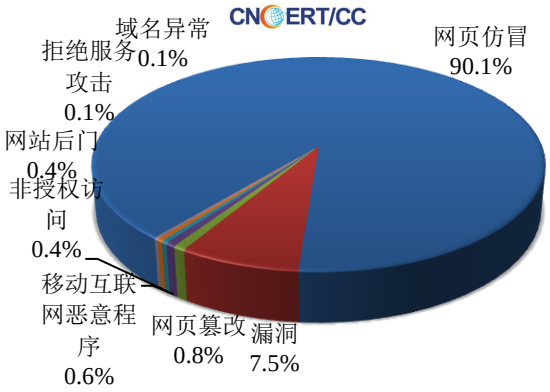
http://www.cnvd.org.cn/webinfo/list?type=4

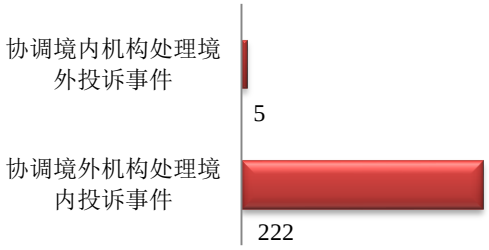
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 788 起，其中跨境网络安全事件 227 起。

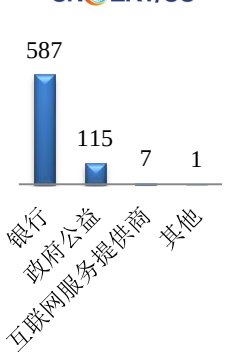
本周CNCERT处理的事件数量按类型分布 (7/16-7/22)



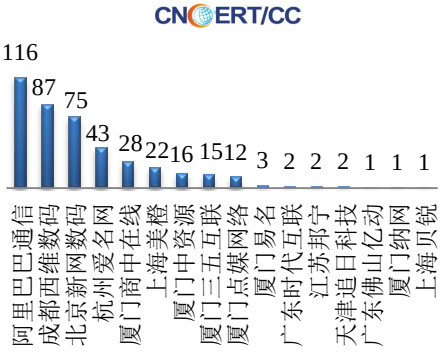


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 710 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 587 起和政府公益仿冒事件 115 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(7/16-7/22)

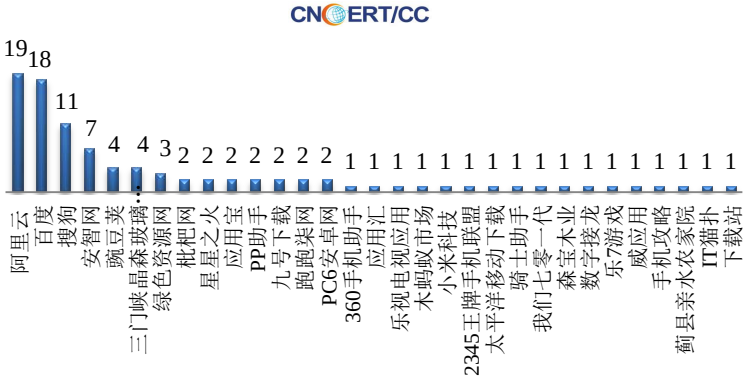


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (7/16-7/22)



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 97 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
(7/16-7/22)



业界新闻速递

1、普京提议与美国成立信息安全合作组织，调查涉美大选指控

HackerNews.cc7 月 17 日消息 在周一备受争议的赫尔辛基峰会期间，俄罗斯总统普京提议与美国成立信息安全合作组织。从表面上看，这将促使美国和俄罗斯结盟。这意味着两国将形成非常奇怪的关系。就在几天前，美国司法部还以 2016 年民主党全国委员会遭黑客攻击为由， 起诉了俄罗斯的 12 名情报官员。但无论如何，俄罗斯总统都试图重启美俄之间关于信息安全事务的合作讨论。对任何关心美国信息安全利益的人来说，这样的提议都将是全球两个大国领导人之间令人困惑的亲密关系的最糟糕结局目前还不清楚，美国能否从这样的协议中获利。美国可能会从中受到损失，因为俄罗斯仍然有兴趣去影响美国大选 。普京在赫尔辛基的言论表明，这种行为的精神依然存在，尽管可能受到了误导。

2、新加坡遭严重网络安全攻击：150 万患者资料被泄露

中新网 7 月 21 日消息 据新加坡《联合早报》报道，新加坡遭受历来最大规模的严重网络安全攻击，150 万名在 2015 年 5 月 1 日至今年 7 月 8 日之间，到新加坡保健服务集团属下的医院和诊所看病的门诊病患个人资料遭网络黑客盗取。调查显示，黑客的攻击行动经过蓄意和精密筹划，先从新保集团的电脑侵入，植入恶意软件后，有目标地攻击新保集团数据库中的具体个人资料，直接和不断地试图盗取和复制总理李显龙的个人医疗记录并成功得逞。此外，患者的姓名、生日、身份证号码和地址等被泄露，其中更有约 16 万人的门诊开药记录也被偷。据悉，新保集团将通过手机简讯和信件联络这 150 万名受影响的患者，他们的其他病历资料没有被盗取，其他公共医疗机构数据库也不受影响。

3、遭黑客攻击隐忧尚存 日本约 6 成地方政府网站安全加密措施落后

环球网 7 月 16 日消息 根据日本一项民间调查，日本全国 6 成地方政府对作为官网安全对策之一的“https

加密”应对落后，网站用户的通信内容有被怀恶意的黑客盗看的隐忧。在日本中央政府 6 月公布的安全对策标准修正案中，写入了中央省厅网站“有义务”实行 https 加密。预计今后也将敦促地方政府网站采取措施。被加密的网址前缀有“https”。未采取加密的情况下，存在输入网页的内容被黑客读取，或被诱导至窃取个人信息的“假网站”的隐忧。据称，若在外使用信用度可疑的无限局域网，风险较高。

4、黑客窃取俄罗斯银行近百万美元

cnBeta.COM7 月 20 日消息 黑客组织 MoneyTaker 本月初从俄罗斯 PIR Bank 窃取了大约 91 万美元。黑客对 PIR Bank 的攻击始于五月，他们首先入侵了银行分支的一个路由器，将其作为入口访问了银行的本地网络。当 MoneyTaker 入侵了 PIR Bank 主网络之后他们设法获得了 Automated Work Station Client of the Russian Central Bank（AWS CBR）访问权限，生成了付款单，将钱转到提前准备好的钱骡子账号。7 月 4 日晚上，当银行雇员发现大笔未经授权的交易之后，他们要求监管机构屏蔽 AWS CBR 数字签名密钥，但他们未能及时阻止资金转移。大部分钱当天被转到了银行卡内并被钱骡子立即取出。攻击者使用了多种恶意程序，其中一种是 MoneyTaker v5.0，大部分恶意程序只存在内存里不会保存到硬盘内。

5、西班牙电信（Telefónica）因一个漏洞暴露了数百万用户的完整个人数据

黑客视界 7 月 18 日消息 据 El Espanol 报道，西班牙电信（Telefónica）在 7 月 16 日凌晨被西班牙消费者协会 FACUA 发现存在一个安全漏洞。透过这个漏洞能够访问数百万用户的完整个人数据，这意味着这些数据可能早已经被置于泄露的边缘。Telefónica 告诉该报，他们在接到这一通知后，立即对该漏洞进行了修复。另外，也向有关当局进行了报告。截至到目前为止，还没有发现任何由于数据泄露导致的欺诈行为。El Espanol 称，因为该漏洞而可能遭到泄露的数据包括用户的个人身份信息和支付卡信息，并且漏洞极其易于利用，即使是不具备高技术水平的入侵者也能够访问对它们进行访问。暴露给黑客的信息包括固定电话和移动电话用户的全名、国家身份证号码、家庭住址、银行记录和通话记录，而所有这些数据都可以以电子表格的形式下载。

6、100 余家车厂机密数据泄漏，特斯拉丰田福特未能幸免

雷锋网 7 月 22 日消息消息 7 月 22 日，据外媒报道，网络安全公司 UpGuard 的安全研究员报告称，100 多家车厂的机密数据被泄露，包括通用汽车、菲亚特克莱斯勒、福特、特斯拉、丰田、蒂森克虏伯、大众等。数据泄漏的源头都指向了这些车厂的共同服务器提供商 Level One Robotics，涉及机密文件 47000 个，泄露的数据包括上述车厂的发展详细蓝图的产品设计图表、消费者发票合约信息、工作研发计划等一系列机密信息。据安全研究员分析，上述服务器使用了一种用于备份大型数据集的通用文件传输协议 rsync，由于没有设定任何安全密码保护措施，通过该传输协议，用户可无障碍访问其中的隐私数据，而且，连接到 rsync 端口的任何客户端都有权下载数据。7 月 10 日，Level One 采取断网脱机的方式暂时切断了此次数据库泄露的路径。

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：吕志泉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158