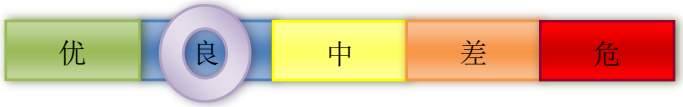
国家互联网应急中心

2018 年第 26 期

6 月 25 日-7 月 1 日

网络安全信息与动态周报

本周网络安全基本态势

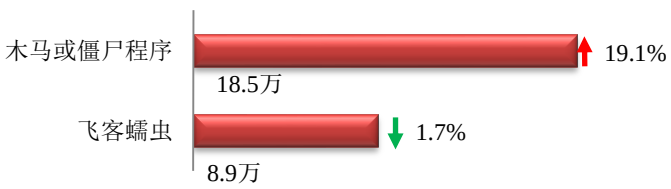


境内感染网络病毒的主机数量	•27.4万	↑ 0.7%
境内被篡改网站总数 其中政府网站数量	•803 •30	↓ 22.3% ↓ 6.3%
境内被植入后门网站总数 其中政府网站数量	•774 •15	↑ 17.3% ↓ 28.6%
针对境内网站的仿冒页面数量	•1169	↑ 21.9%
新增信息安全漏洞数量 其中高危漏洞数量	•285 •107	↑ 31.3% ↑ 55.1%

═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

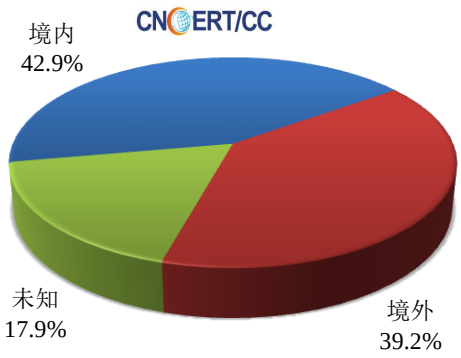
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 27.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 18.5 万以及境内感染飞客（conficker）蠕虫的主机约 8.9 万。

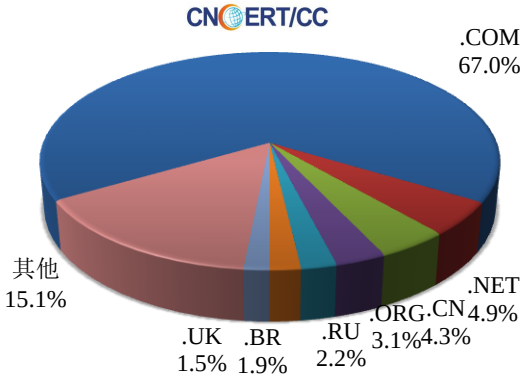


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 324 个，涉及 IP 地址 17172 个。在 324 个域名中，有 39.2%为境外注册，且顶级域为.com 的约占 67.0%；在 17172 个 IP 中，有约 27.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 44 个 IP。

本周放马站点域名注册所属境内外分布
(6/25-7/1)



本周放马站点域名所属顶级域的分布
(6/25-7/1)



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。

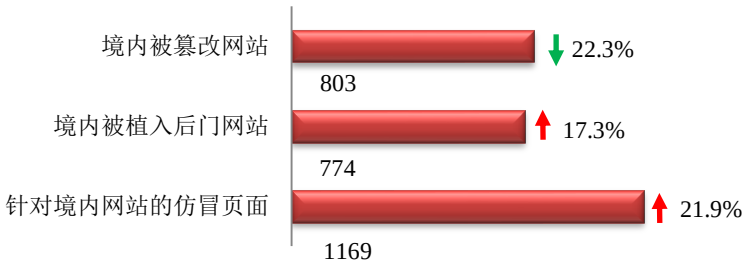
ANVA恶意地址黑名单发布地址

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。

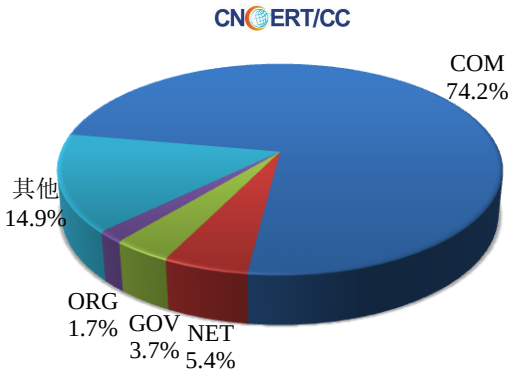
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 803 个；境内被植入后门的网站数量为 774 个；针对境内网站的仿冒页面数量为 1169。

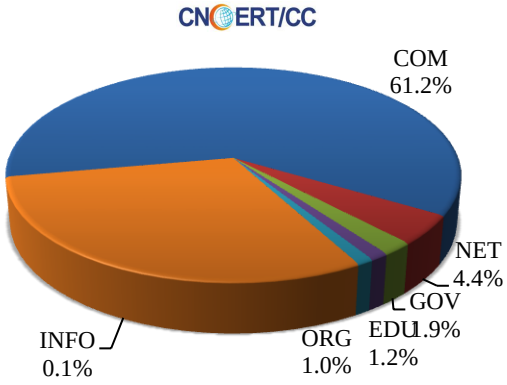


本周境内被篡改政府网站（GOV 类）数量为 30 个（约占境内 3.7%），较上周环比下降了 6.3%；境内被植入后门的政府网站（GOV 类）数量为 15 个（约占境内 1.9%），较上周环比下降了 28.6%；针对境内网站的仿冒页面涉及域名 415 个，IP 地址 220 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(6/25-7/1)

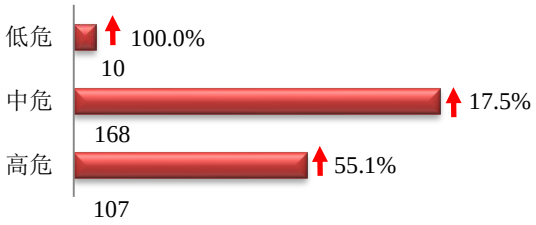


本周我国境内被植入后门网站按类型分布
(6/25-7/1)

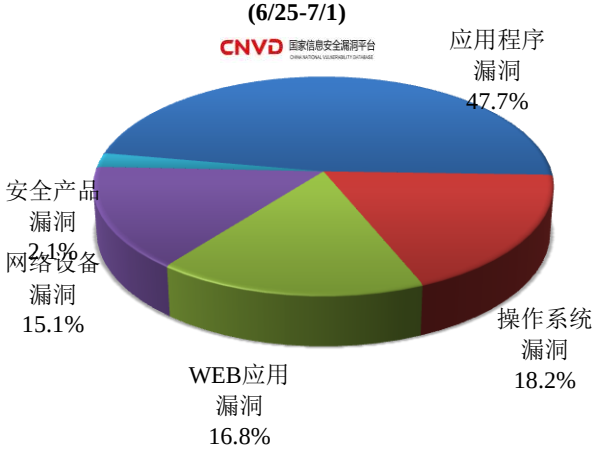


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 285 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
(6/25-7/1)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是操作系统漏洞和 WEB 应用漏洞。

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

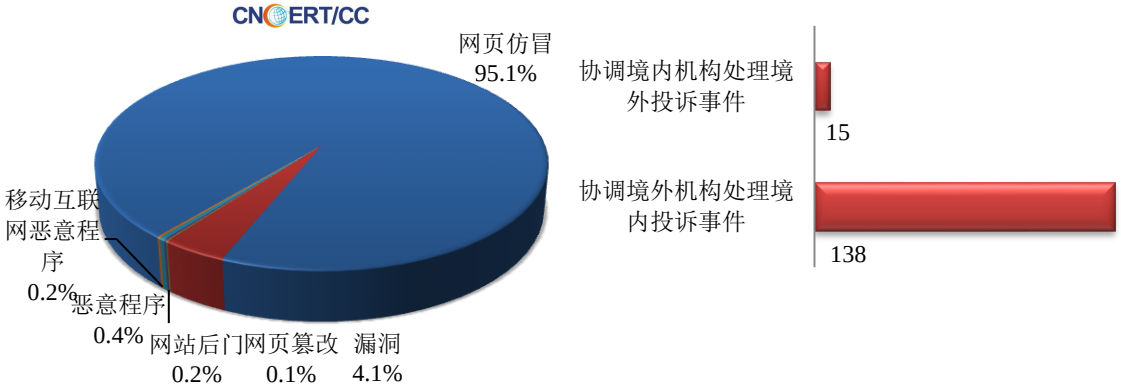
http://www.cnvd.org.cn/webinfo/list?type=4

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

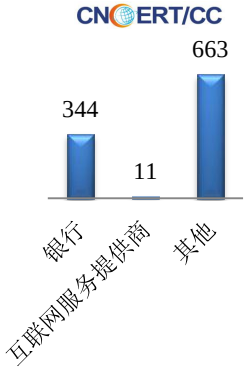
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 1072 起，其中跨境网络安全事件 153 起。

本周CNCERT处理的事件数量按类型分布 (6/25-7/1)

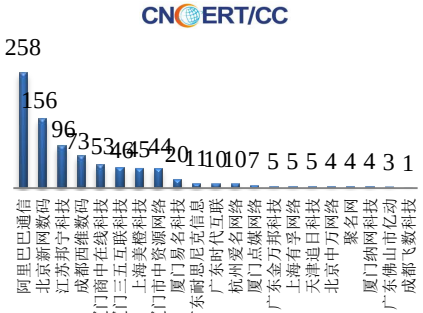


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1018 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 344 起和互联网服务提供商仿冒事件 11 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(6/25-7/1)

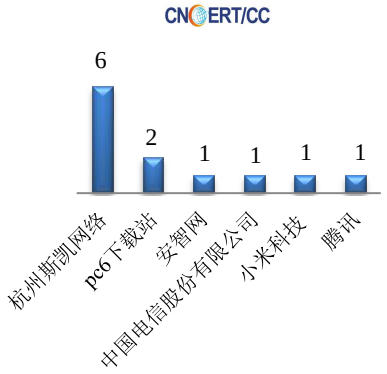


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (6/25-7/1)



本周，CNCERT 协调 6 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 12 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
(6/25-7/1)



业界新闻速递

1、公安部对网络安全等级保护条例征意见 鼓励利用人工智能等技术

证券时报网 6 月 27 日消息 6 月 27 日，公安部就《网络安全等级保护条例（征求意见稿）》公开征求意见。征求意见稿指出，各级人民政府鼓励扶持网络安全等级保护重点工程和项目，支持网络安全等级保护技术的研究开发和应用，推广安全可信的网络产品和服务。鼓励利用新技术、新应用开展网络安全等级保护管理和技术防护，采取主动防御、可信计算、人工智能等技术，创新网络安全技术保护措施，提升网络安全防范能力和水平。

2、美国参议院推进“网络外交法案”，网络空间办公室或将重启

E 安全 6 月 27 日消息 美国参议院外交关系委员会于 2018 年 6 月 26 日通过“网络外交法案”，该法案提出在美国国务院内设立“网络空间和数字经济办公室”，实际上是以此名重启美国务院网络空间办公室。“网络外交法案”提出，“网络空间和数字经济办公室”须由一名由参议院确认的国务院高级官员领导国务院的网络安全事务，该办公室负责人将拥有大使的级别和地位，负责领导美国国务院的网络空间外交工作。法案鼓励美国总统在国会的监督下促成网络空间的国际协议，并要求制定美国国际网络空间政策战略。这项法案的其它要求包括，与其它“志同道合的民主国家”建立信息共享和外交关系，并开发新产品和技术用以保护并加强美国互联网基础设施的安全性。此外，该法案要求美国政府问责局（GAO）向国会报告美国在网络空间面临的国际威胁、外交努力是否有助于保护美国公民的个人敏感信息以及向政策制定者提供保护此类信息的建议。

3、美国佛罗里达州通过设立新职位来监督该州的加密货币行业

cnBeta.COM6 月 27 日消息 据 Coindesk 最新消息，美国佛罗里达州财务长 Jimmy Patronis 周二在一份声明中表示，该州决定通过设立一个新的职位来监督加密货币行业。Patronis 解释说，新的监管人员将负责执行适

用的法规，以保护投资者免受潜在的恶意行为者的伤害。Patronis 指出：“当涉及到加密货币时，佛罗里达州不能再一直处于观望状态，我已经指示我的办公室工作人员设立一个职位，以监督当前的证券和保险法适用于初始投币产品（ICO）和加密货币，以及塑造未来的这些规定。”Patronis 还表示，该职位是为了防止任何形式的剥削性投资。虽然目前尚不清楚这个职位何时会被填补 - 或者由谁来承担，Patronis 表示要采取的步骤是必要的步骤。

4、影响司法调查：多地监管机构要求豁免欧盟数据新规

新浪网 6 月 26 日消息 北京时间 6 月 26 日早间消息，监管部门官员对路透社表示，北美、英国和亚洲的金融监管机构正紧急寻求关于欧盟最新数据保护规定的豁免，以免这项规定不利于跨境的案件调查。这些官员警告，如果欧盟未能明确将市场监管部门排除在欧盟“通用数据保护条例”（GDPR）之外，那么可能会不利于涉及操纵市场和反欺诈的国际调查和司法行动。GDPR 加强了欧盟内部的个人数据隐私保护，让消费者对自己的个人信息拥有更大的控制权。政府官员和法律专家表示，新规定还对出于“公众利益”的跨境个人数据传输进行了限制，对其使用施加了新条件，包括引入额外的隐私保护措施。监管机构担心，在没有豁免的情况下，跨境的信息共享可能遇到问题，欧盟可能会认为，一些国家和地区的隐私保护措施没有达到欧盟要求的水平。消息人士表示，为了抵御这方面的风险，这些监管机构正敦促总部位于布鲁塞尔的欧盟数据保护委员会（EDPB）正式拿出“行政安排”，书面澄清出于公众利益的行为是否可以获得豁免，以及跨境信息共享应当如何操作。

5、美国电信运营商 AT&T 被曝协助 NSA 监控网络流量

E 安全 6 月 28 日消息 美国调查新闻网站 The Intercept 的一份新报告，揭示了美国国家安全局（NSA）和电信服务提供商 AT&T 之间的密切关系。The Intercept 在美国找到了 8 处设施，它们是 AT&T 用来跟 NSA 进行合作的枢纽。该网站最早于 2017 年在曼哈顿下城区找到了第一个潜在的枢纽。报告揭示，AT&T 在美国的 8 处数据设施都被 NSA 视为具有重要价值的站点，因为它们给予后者直接访问经由此地的原始数据的“主干”权限，其中包括电子邮件、网页浏览记录、社交媒体以及其他所有形式的未加密网络活动。NSA 把 AT&T 的这 8 处设施用于一项代号为“FAIRVIEW”的监控行动，《纽约时报》此前曾对该项目进行过报道。FAIRVIEW 在 1985 年首次启动，“涉及接入国际通信线缆、路由器和交换机”，而且只跟 AT&T 直接合作，并不牵涉美国其他大型移动运营商。AT&T 深度参与 NSA 监控项目的行动代号为 SAGUARO。通过该项目获取的短信、电邮和其他网络流量可以通过 XKEYSCORE 进行搜索，这是 NSA 更出名的基于搜索的监控工具之一。

6、美国大数据公司失误泄露 2TB 隐私信息：涉 2.3 亿人

快科技 6 月 28 日消息 据 Wired 报道，本月初曝光的市场和数据汇总公司 Exactis 服务器信息暴露的事情经调查为实。Exactis 采集了大约 3.4 亿条记录，大小 2TB，可能涵盖 2.3 亿人，几乎是全美的上网人口。Exactis 此次的信息泄露并不是黑客撞库引起或者其它恶意攻击，而是他们自己的服务器没有防火墙加密，直接暴露在公共的数据库查找范围内。虽然上述信息中不包含信用卡号、社会保障号码等敏感的金融信息，但是隐私深度却超乎想象，包括一个人是否吸烟，他们的宗教信仰，他们是否养狗或养猫，以及各种兴趣，如潜水和大码服装，这几乎可以帮助构建一个人的几乎完整“社会肖像”。目前，Exactis 已经对数据进行了加密防护。

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：肖崇蕙

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158