国家互联网应急中心

网络安全信息与动态周报

2017 年第 29 期

7 月 10 日-7 月 16 日

CNCERT/CC

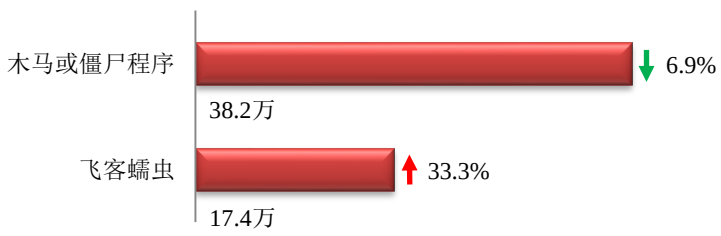
本周网络安全基本态势

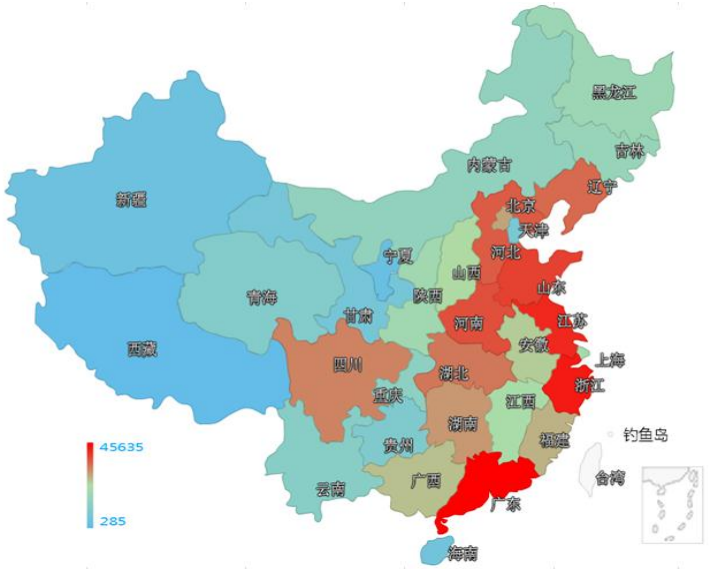
境内感染网络病毒的主机数量	•55.6万	↑ 2.7%
境内被篡改网站总数 其中政府网站数量	•2966 •53	↑ 151.4% ↑ 10.4%
境内被植入后门网站总数 其中政府网站数量	•1127 •75	↓ 37.8% ↓ 28.6%
针对境内网站的仿冒页面数量	•335	↑ 34.0%
新增信息安全漏洞数量 其中高危漏洞数量	•413 •178	↑ 34.1% ↑ 58.9%

= 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 55.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 38.2 万以及境内感染飞客（conficker）蠕虫的主机约 17.4 万。





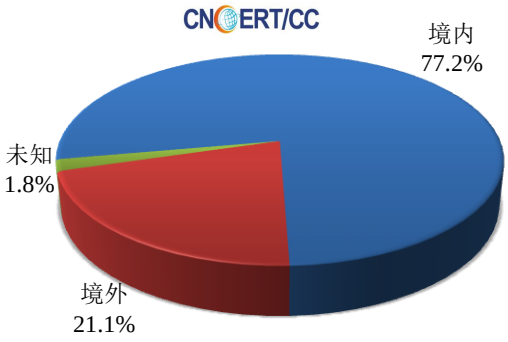
木马或僵尸程序受控主机在我国大陆的分布情况如左图所示，其中红色区域是木马和僵尸程序感染量最多的地区，排名前三位的分别是广东省、浙江省和江苏省。

TOP3

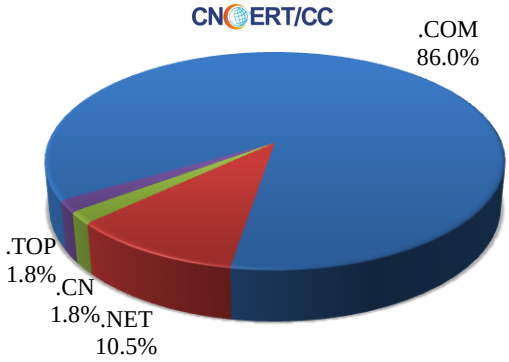
广东省	• 约4.6万个（约占中国大陆总感染量的11.9%）
浙江省	• 约4.1万个（约占中国大陆总感染量的10.7%）
江苏省	• 约3.1万个（约占中国大陆总感染量的8.1%）

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 57 个，涉及 IP 地址 70 个。在 57 个域名中，有 21.1%为境外注册，且顶级域为.com 的约占 86.0%；在 70 个 IP 中，有约 1.4%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 2 个 IP。

本周放马站点域名注册所属境内外分布
(7/10-7/16)



本周放马站点域名所属顶级域的分布
(7/10-7/16)



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。

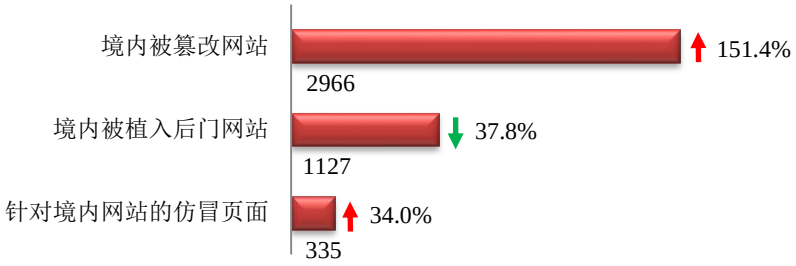
ANVA恶意地址黑名单发布地址

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。

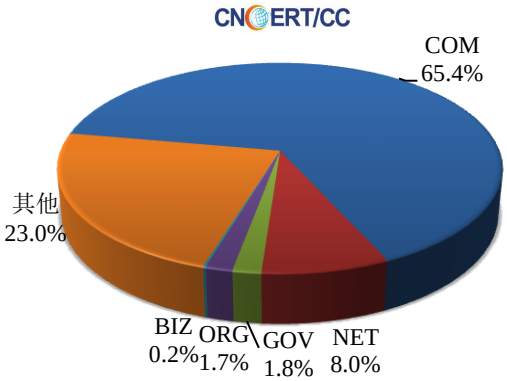
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2966 个；境内被植入后门的网站数量为 1127 个；针对境内网站的仿冒页面数量为 335。

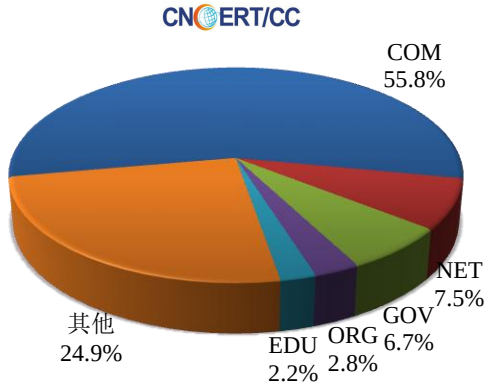


本周境内被篡改政府网站（GOV 类）数量为 53 个（约占境内 1.8%），较上周环比上升了 10.4%；境内被植入后门的政府网站（GOV 类）数量为 75 个（约占境内 6.7%），较上周环比下降了 28.6%；针对境内网站的仿冒页面涉及域名 283 个，IP 地址 138 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(7/10-7/16)



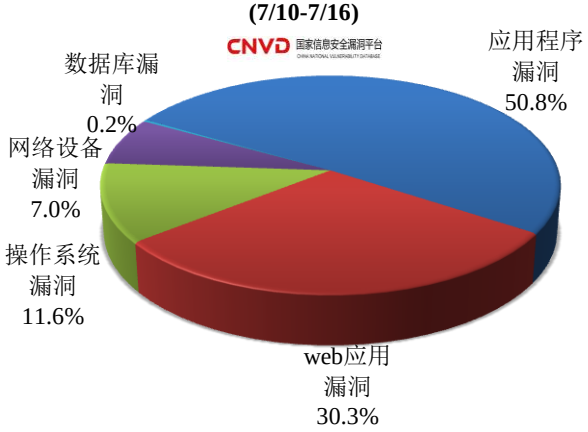
本周我国境内被植入后门网站按类型分布
(7/10-7/16)



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 413 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
(7/10-7/16)



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

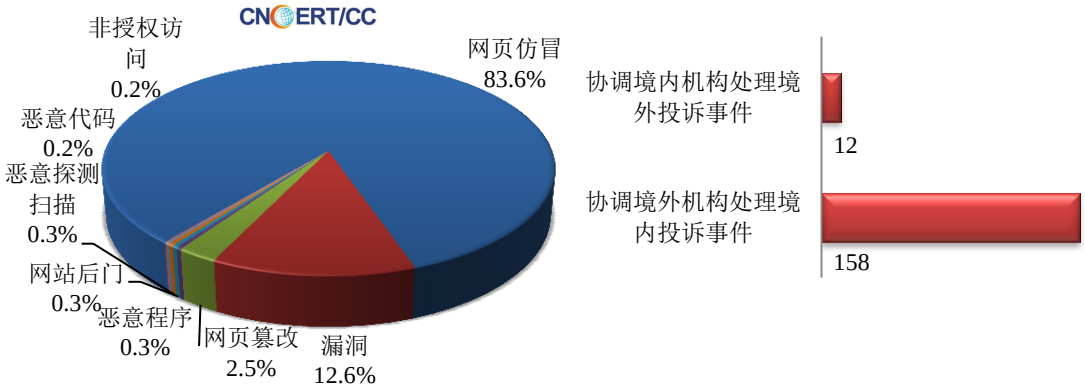
http://www.cnvd.org.cn/webinfo/list?type=4

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

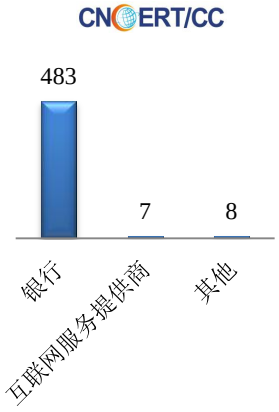
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 596 起，其中跨境网络安全事件 170 起。

本周CNCERT处理的事件数量按类型分布
(7/10-7/16)

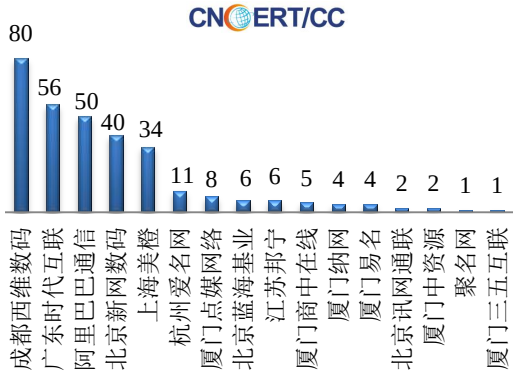


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 498 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 483 起和互联网服务提供商仿冒事件 7 起。

本周CNCERT处理网页仿冒事件数量
按仿冒对象涉及行业统计(7/10-7/16)

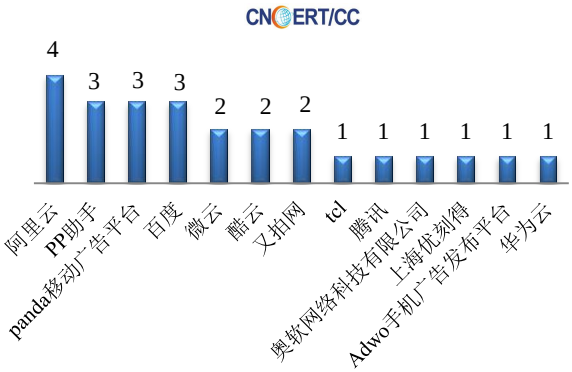


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (7/10-7/16)



本周，CNCERT 协调 13 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 25 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
(7/10-7/16)



业界新闻速递

1、德将推出新网络安全计划 防止黑客入侵航空系统

环球网 7 月 14 日消息 据新加坡《联合早报》7 月 14 日报道，德国军方将展开一项新的网络安全计划，以防止网络黑客入侵航空系统，掌控德国军方飞机。德国航空航天中心此前向德国军方展示，黑客只需利用 5000 欧元的仪器就能控制军方的飞机。因此，德国军方决定制定新的网络安全计划，准备栽培航空网络安全领域的专才，同时加强相关技术研究，为飞机安装防护系统等。据报道，德国军方今年组建了一个新的“网络军团”，将来自各部门的网络安全单位组织起来，这个网络军团也将参与新的航空安全计划。德国航空航天中心发言人说，6 月在慕尼黑联邦国防军大学举行的会议中，确保网络系统可以抵御网络袭击并继续运作是其中一个主要议题。德军也致力于在欧盟和北约组织内解决航空网络问题。

2、日本政府就网络安全开会 将成立指挥中心迎奥运

中新网 7 月 14 日消息 据日媒报道，日本政府 13 日在首相官邸召开由官房长官菅义伟亲自挂帅的网络安全战略总部会议，为修改力争确保互联网环境安全的《网络安全战略》汇总了中期报告。报告称，将在 2018 年度结束前后成立政府指挥中心，应对瞄准 2020 年东京奥运会和残奥会的网络攻击。此外还将新设官民迅速共享安全威胁等信息并处理的机制。报告写明，将讨论为创建便于提供信息的环境而完善法律。目前的战略于 2015 年 9 月在内阁会议上决定。实施期间至 2018 年 9 月，但根据中期报告的新政策也将同步推进。据悉，指挥中心名为“网络安全应对协调中心”，一旦在电力、通信、交通和医疗等重要服务系统发生网络攻击，将立即建议应对方法，与奥组委携手把损失控制在最小程度。奥运之前，将在 2019 年的日本橄榄球世界杯中试用。指挥中心除了安排十余名专职人员外，还将与民间技术人员等 200 人以上建立合作机制。一年内还将构建官民共同汇总与分析信息的机制，暂名为“信息共享与协作网络”，汇集与网络相关的故障与威胁信息。

3、新加坡拟定新网络安全法规，采取积极措施维护国家关键基础设施

HackerNews.cc7 月 13 日消息 据外媒 7 月 10 日报道，新加坡于近期公布了一份新网络安全法规草案，旨在保障国家网络安全、维护关键基础设施（CII）并授权当局履行必要职责，以促进各关键部门共享信息。目前，新加坡政府已列出 11 个被认为拥有 CII 的部门，包括水资源、医疗、海运、媒体、信息、能源与航空等，这些公共部门本身就是 CII 的一部分。知情人士指出，由于新加坡是全球遭受网络攻击最为严重的数字连接国家之一，因此其 CII 将受到巨大影响。CSA 行政长官 David Koh 指出，新加坡目前的网络安全立法主要侧重于计算机网络犯罪行为。为监督国家持续发展网络安全景观，新加坡需制定一个更全面的法案法规进行约束。而此次拟定的法案关键组成部分则是针对 CII 所有者进行监管，规定了 CII 提供商在履行必要职责的情况下定期评估 CII 风险，遵守业务守则。法案还规定，CII 所有者将被要求执行必要机制与流程，以检测关键信息的网络安全威胁。目前，关于该法案的公众意见将于 2017 年 8 月 3 日前提交至 CSA。

4、勒索软件 Petya 攻击后，北约加强乌克兰网络防御支持

HackerNews.cc7 月 15 日消息 据外媒报道，继乌克兰上月遭受勒索软件 Petya 肆意袭击后，北约加强了对

乌克兰网络防御的支持。7 月 10 日，乌克兰总统波罗申科在与北约联合主办的会议上发布声明，指出乌克兰将通过与北约的密切合作深化国防与安全领域的各项改革，加强国家网络安全防御体系。“关键基础设施”是任何一个国家在经济上最为敏感的要素之一。2017 年 6 月，乌克兰遭受勒索软件 Petya 攻击后，导致交通、银行与电力基础设施在补救与恢复工作中造成无法估量的成本代价。乌克兰关键基础设施的维护相比其他国家较为完善，因此如果同样的攻击活动转移目标，后果将不堪设想。北约秘书长 Jens Stoltenberg 表示，北约将继续帮助乌克兰加快国防与安全领域的改革，并协助乌克兰调查 Petya 攻击活动的幕后黑手。2014 年 12 月，北约就已成立网络防御信托基金会，旨在提供必要支持、发展防御型 CSIRT 技术能力。

5、FBI 与 DHS 发布联合警报：APT 组织已成功渗透美国核设施系统

HackerNews.cc7 月 12 日消息 据外媒 7 月 10 日报道，美国国土安全部（DHS）与联邦调查局（FBI）上周发布联合警报，指出黑客组织早于今年 5 月成功渗透美国等国核电站、工厂与能源设施的企业网络。据《纽约时报》透露，由于该报告并未提供黑客攻击动机，因此调查人员尚未掌握足够证据证明攻击者是否完全掌控目标网络、访问控制系统，也暂时无法对黑客使用的恶意软件/工具进行隔离与分析。调查显示，黑客组织多数情况下围绕具有关键工控系统直接访问权限的工程师展开网络钓鱼活动。一旦系统遭受破坏，可能导致工厂爆炸、火灾或危险物质泄露等安全事故。分析表明，黑客通过含有恶意软件的 Microsoft Word 文档窃取受害者登录凭据并在目标网络上进行横向传播。此外，黑客还利用安全漏洞攻击受害者访问的合法网站。安全专家猜测，此类事件与境外政府资助的 APT 组织有关，攻击者策略、技术与流程（TTP）均效仿了以往入侵能源行业的 APT 组织。目前，美国国土安全部（DHS）已将关键基础设施的网络攻击视为国家必须面对的头等安全挑战之一。

6、印度发生最大规模数据泄漏事件 1 亿多用户信息被曝光

新浪网 7 月 12 日消息 北京时间 7 月 11 日晚间消息，针对所谓的“用户数据泄露”事件，印度电信运营商 Reliance Jio 日前表示，正在对此展开调查。近日，有印度媒体发现，Reliance Jio 的一亿多用户的数据被泄漏到 Magicapk.com 网站上，包括姓名、手机号、电子信箱、SIM 激活日期，甚至还包括 Aadhaar 号码（身份识别信息）。业内人士认为，如果消息属实，这可能是印度电信史上最大规模的用户数据泄漏事件。目前，Reliance Jio 正在调查此事，但已初步表示，Magicapk.com 网站上发布的数据似乎是“不真实的”。Reliance Jio 还称，它们对用户数据采用了最高等级加密，非常安全。但是，已经有许多 Reliance Jio 用户在 Twitter 上抱怨，称自己的个人资料被曝光。此外，一些印度媒体经过调查后也证实，Magicapk.com 上的数据是真实的。对此，Reliance Jio 一发言人称：“针对数据泄露一事，我们已经通知了执法部门，将来我们还会继续跟进。”

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。截止 2016 年，CNCERT 与 69 个国家和地区的 185 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：徐剑

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话： 010-82990158