国家互联网应急中心

网络安全信息与动态周报

2017 年第 39 期

9 月 18 日-9 月 24 日

CNCERT/CC

本周网络安全基本态势

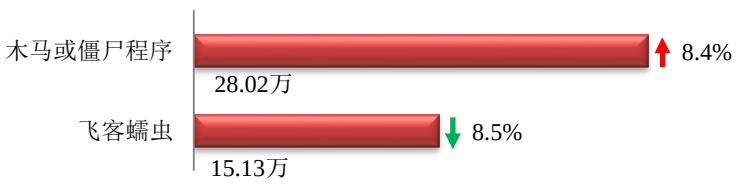
境内感染网络病毒的主机数量	•43.15万	1.8%
境内被篡改网站总数 其中政府网站数量	•1801 •56	12.8% 5.7%
境内被植入后门网站总数 其中政府网站数量	•934 •56	1.9% 3.7%
针对境内网站的仿冒页面数量	•268	9.8%
新增信息安全漏洞数量 其中高危漏洞数量	•325 •129	27.8% 27.5%

v

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*

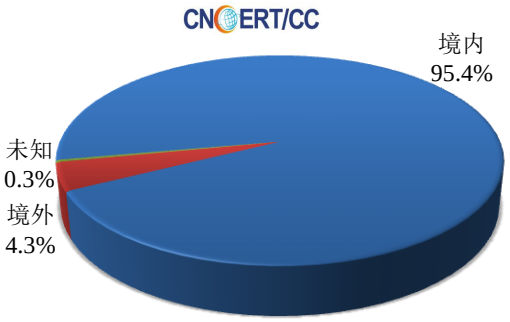
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 43.15 万个，其中包括境内被木马或被僵尸程序控制的主机约 28.02 万以及境内感染飞客（conficker）蠕虫的主机约 15.13 万。

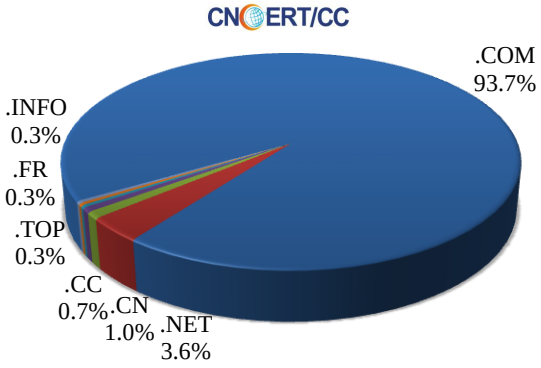


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 302 个，涉及 IP 地址 387 个。在 302 个域名中，有 4.3%为境外注册，且顶级域为.com 的约占 93.7%；在 387 个 IP 中，有约 7.8%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 8 个 IP。

本周放马站点域名注册所属境内外分布
(9/18-9/24)



本周放马站点域名所属顶级域的分布
(9/18-9/24)



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。

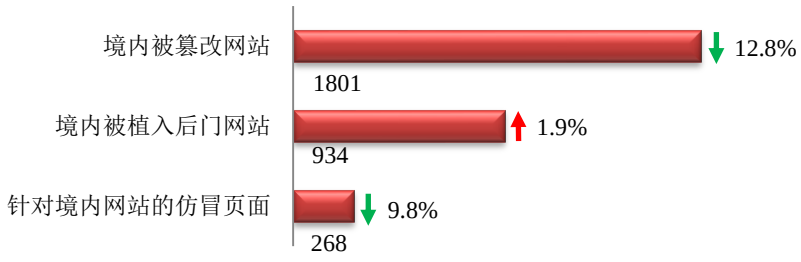
ANVA恶意地址黑名单发布地址

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。

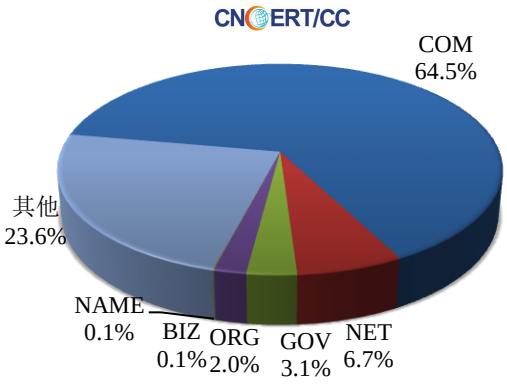
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1801 个；境内被植入后门的网站数量为 934 个；针对境内网站的仿冒页面数量为 268。

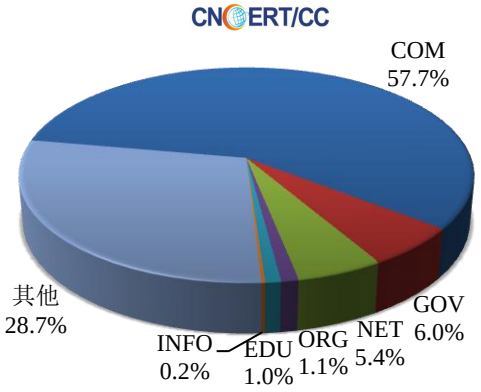


本周境内被篡改政府网站（GOV 类）数量为 56 个（约占境内 3.1%），较上周环比上升了 5.7%；境内被植入后门的政府网站（GOV 类）数量为 56 个（约占境内 6.0%），较上周环比上升了 3.7%；针对境内网站的仿冒页面涉及域名 206 个，IP 地址 110 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(9/18-9/24)

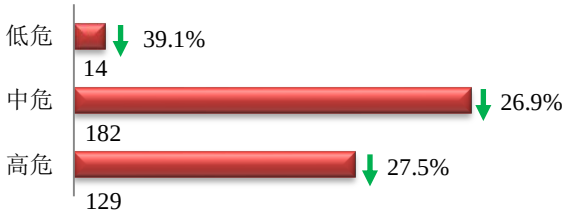


本周我国境内被植入后门网站按类型分布
(9/18-9/24)

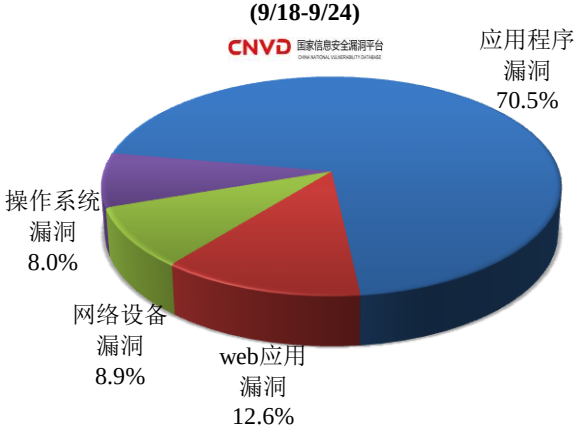


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 325 个，信息安全漏洞威胁整体评价级别为高。



本周CNVD收录漏洞按影响对象类型分布
(9/18-9/24)



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。

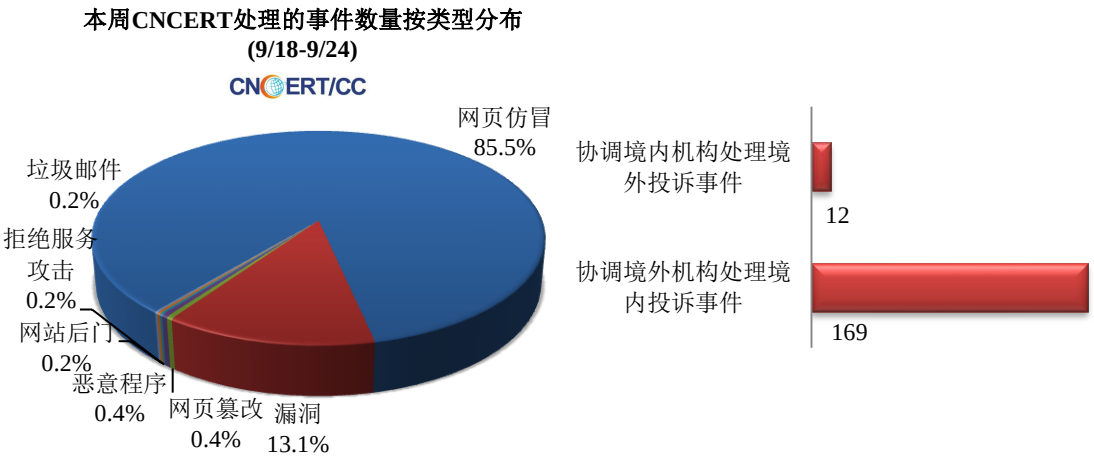
CNVD漏洞周报发布地址

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。

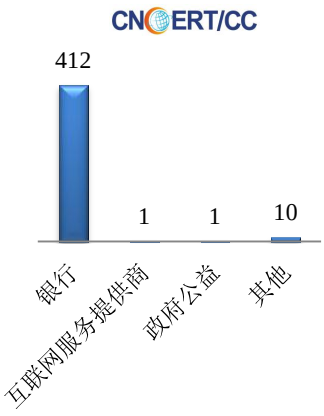
本周事件处理情况

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 496 起，其中跨境网络安全事件 181 起。

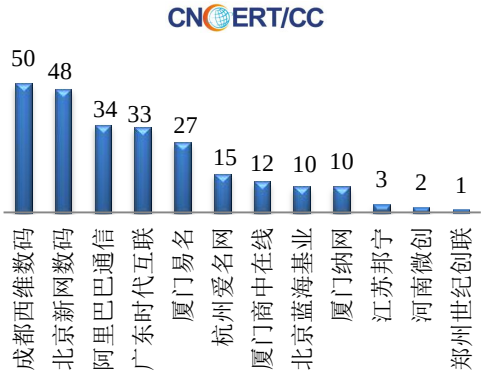


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 424 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 412 起和互联网服务提供商仿冒事件 1 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(9/18-9/24)

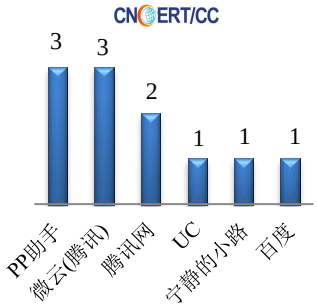


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (9/18-9/24)



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 11 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 (9/18-9/24)



业界新闻速递

1、英国 NCC 为加强网络威胁保障，推出 CENTA 计划提供安全支持

HackerNews.cc9 月 18 日消息 英国国家计算中心（NCC）为保障政府、央行、监管机构等多家组织的网络安全，特创立新一代威胁保障中心（CENTA）、聘请三家银行网络专家 Phillip Larbey、Anthony Long 与 Fiona Paterson 就网络弹性与最佳实践方案提供可靠建议。知情人士透露，CENTA 计划主要为境外央行与监管机构提供全球网络安全咨询服务、协助有关机构对网络弹性的准备、设计、实施与支持，以及网络安全测试监管制度的设计与发展。此外，该计划还将为各机构提供培训、网络管理测试、根源分析、纠正修复与安全审核等项目。Larbey 表示：“我们将与地缘政治论坛合作，为政府部门、中央银行、监管机构等多家组织提供网络安全咨询与支持，以维护网络安全管理最高标准。而这些使命将是 NCC 的一剂补药，因为 NCC 在过去网络动荡的一年里，已收到三次重大合同取消后的利润警告。”NCC 网络风险管理与治理总监 Ben Jepson 表示：“政府与监管机构是最具网络威胁的受害组织，而我们创建 CENTA 计划，旨在提供专门的安全咨询服务，以便帮助各机构

提高网络威胁防御能力。”

2、土耳其将推出新的网络安全计划：5 个战略、41 个独立的行动主题

E 安全 9 月 18 日消息 土耳其交通、海事与通信部长 Ahmet Arslan（艾哈迈德·阿尔斯兰）表示，土耳其政府正在规划全新的网络安全综合蓝图，以打击日益严峻的国内及全球威胁。Arslan 本周接受土耳其媒体 Sabah 的采访时表示，“国家网络安全战略与行动计划”（National Cyber Security Strategy and Action Plan）包含 5 个战略目标，41 个独立的行动主题和 167 个实际步骤。Arslan 表示，网络安全委员会目前为止已开展四次会议。土耳其成立国家计算机应急响应中心（简称 USOM）协调公共部门与私营部门共同合作打击网络犯罪，此外土耳其还成立了 720 个以私营部门为基础的计算机应急响应小组（简称 CERT）。此外，土耳其还计划拓宽国家计算机应急响应中心和计算机应急响应小组的行动范围。国家计算机应急响应中心将成为管理所有计算机应急响应小组的伞式机构。土耳其目前正在实施 KamuNet 项目。通过该项目，土耳其将建立闭路虚拟网络，方便公共机构之间传输数据，同时防止数据传输免受外部干扰。

3、新加坡成为全球网络攻击发起国的首选

和讯网 9 月 22 日消息 以色列数据安全公司 Check Point 的数据显示，新加坡已经超越了包括美国、俄罗斯以及中国在内的一众国家，成为了全球黑客发起网络攻击的首选国。该公司每天平均能追踪 8 百万到 1 千万次的网络攻击事件。Check Point 亚太区发言人 Eying Wee 说：“新加坡在网络攻击国中排名第一并非异常。”新加坡的互联网流量很多都来自其他国家。她表示，这意味着一些显示由新加坡发起的网络攻击，实则来自其他国家。新加坡政府发言人在一封电子邮件中说：“作为高度互联互通的商业中心，新加坡无疑是网络犯罪分子的有力吸引目标。对于维护网络安全标准，新加坡有必要采取措施来保护系统和数据。”今年早间，新加坡军方成立了网络防御部队，政府起草立法新网络安全法，5 月份，新加坡大部分公务员停止了从工作电脑访问互联网途径。这一切都旨在帮助企业保护信息基础设施。

4、继 1.4 亿美国用户遭殃后，Equifax 让 40 万英国人的信息也面临风险

雷锋网 9 月 22 日消息 泄露了 1.4 亿美国用户信息的 Equifax，这两天又被曝出其在英国也遇到了麻烦，40 万英国人民的个人信息也岌岌可危。Equifax 原本和另外一家英国本土的征信公司“TDX”共用一个网上平台，当 Equifax 发生泄漏事件之后，他们才在业务上完全分开，但是同用一个平台的“TDX”还是受到了影响。调查显示，存在一些未被授权的途径可以访问到某些英国用户的个人信息，由于”进程错误“（process failure），英国的一些数据被存储在美国，这些数据包括姓名，出生日期，电子邮件地址，电话号码，Equifax 也确认这些数据中不包括任何的居民地址信息，密码信息或是一些金融信息。经过初步评估，Equifax 已经确定，将会联系这 40 万左右的英国用户，给他们提供适当的建议和一系列服务，好让他们放心。据称，被盗的英国消费者数据不包含任何一个 Equifax 公司的客户。

5、伊朗黑客组织 APT33 瞄准多国航空国防能源机构展开新一轮网络攻击活动

HackerNews.cc9 月 22 日消息 美国网络安全公司 FireEye 研究人员近期发现伊朗黑客组织 APT33 似乎开始瞄准多国航空、国防与能源设施展开新一轮网络攻击活动。目前，受影响机构包括美国航空航天公司、沙特阿

拉伯商业集团，以及韩国石油石化公司。黑客组织 APT33 至少于 2013 年就已针对多国关键基础设施、能源与军事部门发起攻击，旨在收集情报、窃取商业机密信息。调查显示，黑客组织 APT33 通过发送附带恶意链接的网络钓鱼邮件感染目标设备，其主要使用的恶意软件包括 DROPSHOT（病毒传播器）、SHAPESHIFT（恶意软件删除器）与 TURNEDUP（自定义后门）。有趣的是，虽然该组织仅仅利用 DROPSHOT 传播 TURNEDUP 后门，但他们却在攻击活动中发现多款 DROPSHOT 释放样本。此外，恶意软件 SHAPESHIFT 则主要用于擦除磁盘信息并删除文件记录的操作。

6、新型 Android 恶意软件 Red Alert 2.0 已感染逾 60 款银行与社交媒体应用

HackerNews.cc9 月 20 日消息 据外媒 9 月 19 日报道，网络安全公司 SyfLabs 研究人员近期发现一款新型 Android 银行恶意软件 Red Alert 2.0，允许黑客窃取用户敏感信息、劫持短信邮件，并阻止与银行、金融机构相关的所有来电呼叫。目前，Red Alert 2.0 已感染 Google Play 商店上超过 60 款银行与社交媒体应用。不过，与其他 Android 木马不同的是，该恶意软件是由开发人员从零开始编写。如果目标设备的 C&C 服务器被关闭时，该恶意软件可以通过 Twitter 保存所有数据信息。然而，当设备无法连接到硬编码的 C2 时，它可以从 Twitter 帐户中重新检索一台新 C2 服务器进行连接。研究人员表示，这也是他们第一次从移动设备的恶意软件中发现此类银行木马。SfyLabs 首席执行官兼创始人 Cengiz Han Sahin 表示，虽然 Red Alert 2.0 的开发人员现在只以 500 美元的价格出售该恶意软件，但他们日前仍在为其新添更多功能，包括远程操控受感染设备。目前，该恶意软件主要影响 Android Marshmallow 以及之前版本。

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：徐丹丹

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158