国家互联网应急中心

网络安全信息与动态周报

2019 年第 38 期

9 月 16 日-9 月 22 日

CNCERT/CC

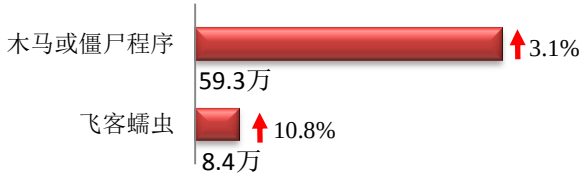
本周网络安全基本态势

境内感染网络病毒的主机数量	•67.8 万	4.0%
境内被植入后门网站总数 其中政府网站数量	•3234 •41	9.9% 36.7%
针对境内网站的仿冒页面数量	•54	3.8%
新增信息安全漏洞数量 其中高危漏洞数量	•405 •88	11.0% 1.1%

=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

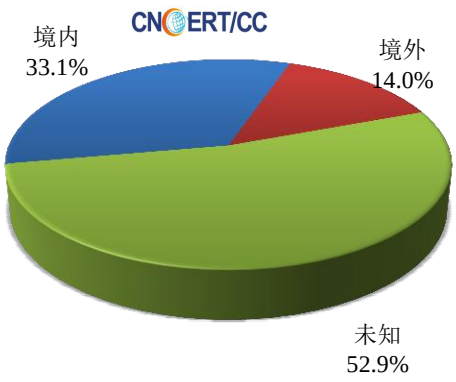
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 67.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 59.3 万以及境内感染飞客（conficker）蠕虫的主机约 8.4 万。

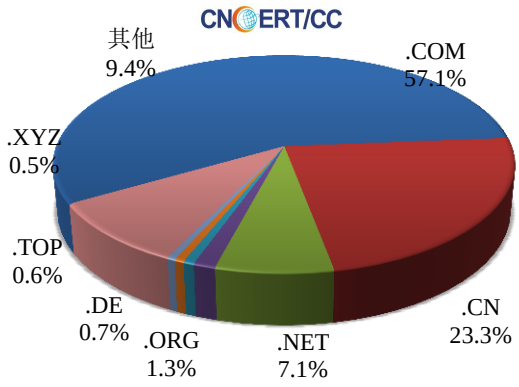


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 1197 个，涉及 IP 地 2233 个。在 1197 个域名中，有 14.0%为境外注册，且顶级域为.com 的约占 57.1%；在 2233 个 IP 中，有约 38.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 366 个 IP。

本周放马站点域名注册所属境内外分布
(9/16-9/22)



本周放马站点域名所属顶级域的分布
(9/16-9/22)



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。

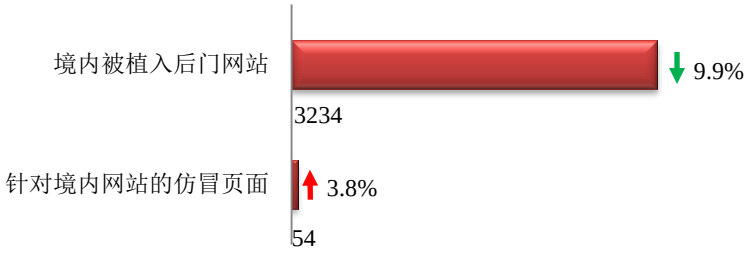
ANVA恶意地址黑名单发布地址

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。

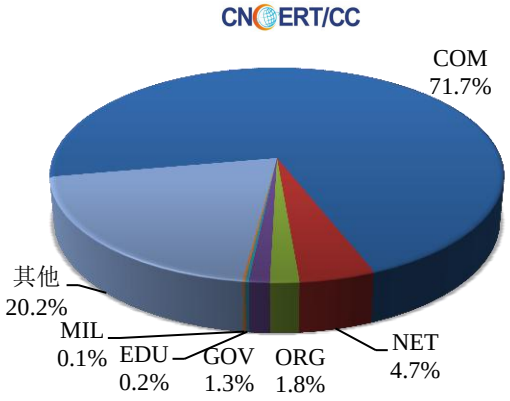
本周网站安全情况

本周 CNCERT 监测发现境内被植入后门的网站数量为 3234 个；针对境内网站的仿冒页面数量 54 个。



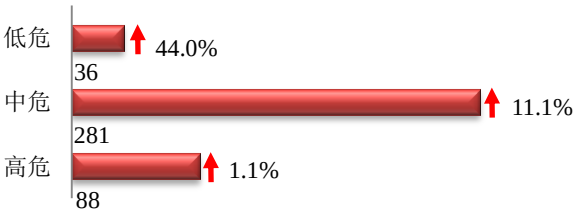
本周境内境内被植入后门的政府网站（GOV 类）数量为 41 个（约占境内 1.3%），较上周环比上升 36.7%；针对境内网站的仿冒页面涉及域名 28 个，IP 地址 29 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被植入后门网站按类型分布
(9/16-9/22)

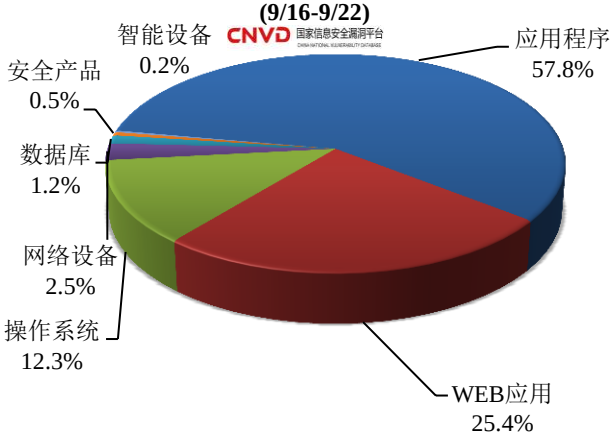


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 405 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
(9/16-9/22)



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。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

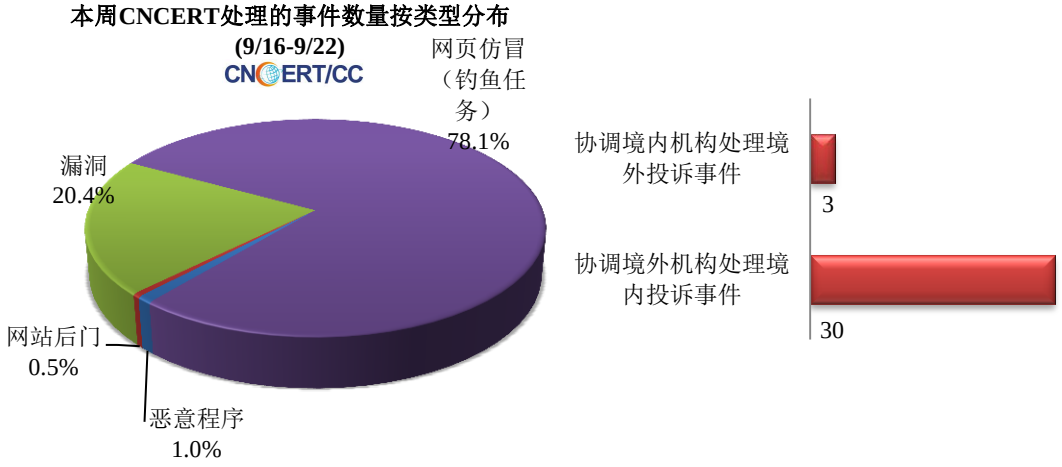
CNVD漏洞周报发布地址

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

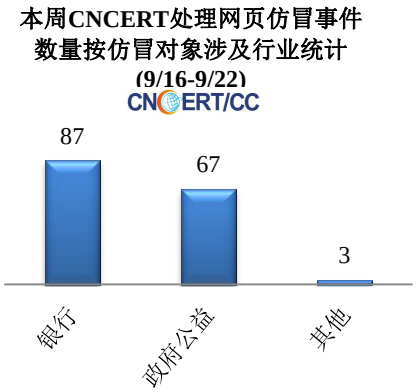
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

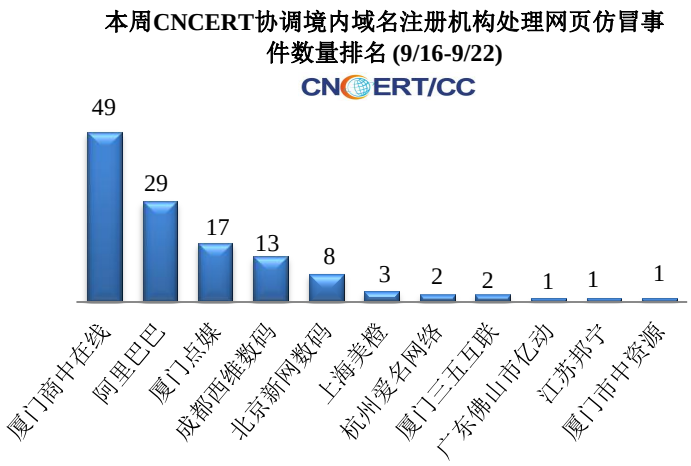
本周事件处理情况

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 201 起，其中跨境网络安全事件 33 起。



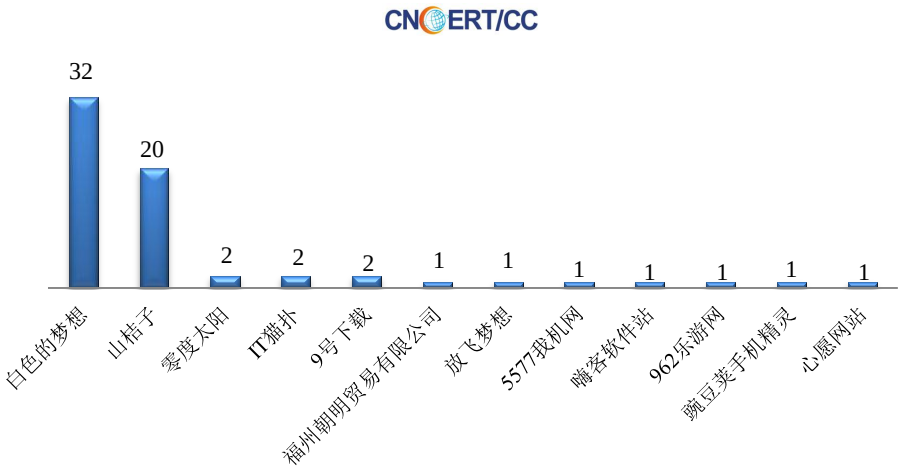
本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 157 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 87 起和政府公益事件 67 起。





本周，CNCERT 协调 12 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 65 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
(9/16-9/22)



业界新闻速递

1、 网信办回应"ZAO"涉嫌违规:已制定法规专项治理

9 月 18 日，北京青年报消息，当日，在国务院新闻办公室召开的新闻发布会上，国家互联网信息办公室副主任刘烈宏回答了记者关于换脸 App“ZAO”的涉嫌违规一事。刘烈宏表示，国家网信办积极支持新技术、新应用的发展。同时，也采取制定法规、专项监管等多项必要措施防范随之带来的风险。

刘烈宏指出，新技术、新应用带来了发展机遇，同时也给网络安全带来了风险和挑战。作为管理部门，国家网信办积极支持新技术、新应用的发展。同时，也采取必要措施防范随之带来的风险。现已经会同有关部门制定出台了《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》《个人信息安全规范》等法规标准，正在制定《网络生态治理规定》，目前在征求意见。

2、信通院发布《中国网络安全产业白皮书（2019 年）》

9 月 19 日中国信通院官网消息，19 日中国信息通信研究院在 2018 国家网络安全宣传周上发布《中国网络安全产业白皮书（2018）》《区块链安全白皮书-技术应用篇》两项最新研究成果，信通院院长刘多对白皮书进行了现场解读。

刘多在解读《中国网络安全产业白皮书（2018）》时指出，坚实的网络安全产业实力，是网络空间繁荣稳定、保障有力的前提和基础。为深入贯彻落实习近平总书记关于网络强国的重要思想，助力网络安全产业创新发展，中国信息通信研究院安全研究所持续开展网络安全产业发展研究，自 2015 年起每年通过白皮书等方式与业界分

享研究成果。本白皮书延续了从规模结构、政府政策、企业发展、技术进展、人才培养等维度对国内外产业进展跟踪分析，同时汇聚业界力量、结合热点趋势，重点对身份管理与访问控制、可管理安全服务、云安全、威胁情报服务、“人工智能+安全”五个领域进行了分析预测，并对产业发展前景进行了展望

3、厄瓜多尔多数公民数据遭泄露 其中包括 670 万儿童

9 月 16 日 ZDNet 消息，由于数据库配置错误，厄瓜多尔大部分人口（包括儿童）的个人记录已在网上曝光。两周前，vpnMentor 安全研究人员 Noam Rotem 和 Ran Locar 发现了这个数据库泄露。

此次泄露的数据库总共包含大约 2080 万个用户记录，这个数据库记录的数量大于该国家的总人口数，其中原因可能来自重复记录或较旧的条目，包含死者的数据。这项数据存储了用户详细信息，如姓名，家庭成员，民事登记数据，财务和工作信息，以及汽车所有权数据。另外，安全研究人员发现整个数据库当中也包含大量儿童信息，有些儿童甚至是今年春季才出生。具体来说，其中包含大约 677 万个 18 岁以下儿童条目。这些条目包含姓名、出生地、家庭住址和性别等信息。

4、Facebook 平台暂停数万个应用 加强用户隐私保护

9 月 20 日《纽约时报》消息，社交网络公司 Facebook 近日表示，其社交网络平台上数万个应用程序已经被暂停使用。针对剑桥分析公司(Cambridge Analytica)丑闻事件，该公司于 2018 年 3 月启动了对其平台上应用开发者的调查。此次暂停使用措施，是正在进行的该调查行动的一部分。

Facebook 称这些被暂停的应用程序与大约 400 名开发者有关，并声称被暂停并不一定表明这些应用程序对用户构成了威胁。

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：郭禹

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315