国家互联网应急中心

网络安全信息与动态周报

2019 年第 37 期

9 月 9 日-9 月 15 日

CNCERT/CC

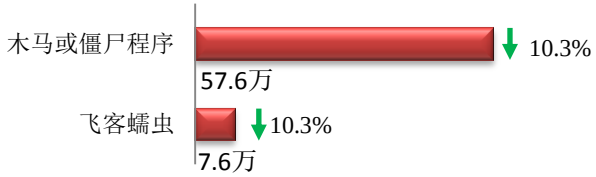
本周网络安全基本态势

境内感染网络病毒的主机数量	•65.2 万	↓ 10.3%
境内被植入后门网站总数 其中政府网站数量	•3590 •30	↑ 7.5% ↓ 9.1%
针对境内网站的仿冒页面数量	•52	↓ 1.9%
新增信息安全漏洞数量 其中高危漏洞数量	•365 •87	↓ 48.5% ↓ 63.9%

═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

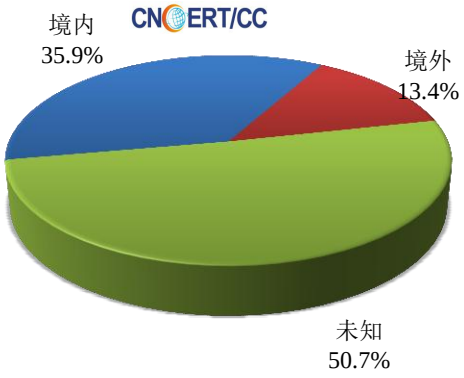
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 65.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 57.6 万以及境内感染飞客（conficker）蠕虫的主机约 7.6 万。

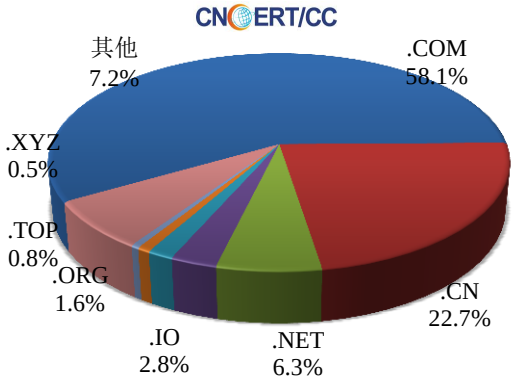


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 1380 个，涉及 IP 地 2441 个。在 1380 个域名中，有 13.4%为境外注册，且顶级域为.com 的约占 58.1%；在 2441 个 IP 中，有约 27.0%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 381 个 IP。

本周放马站点域名注册所属境内外分布
(9/9-9/15)



本周放马站点域名所属顶级域的分布
(9/9-9/15)



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。

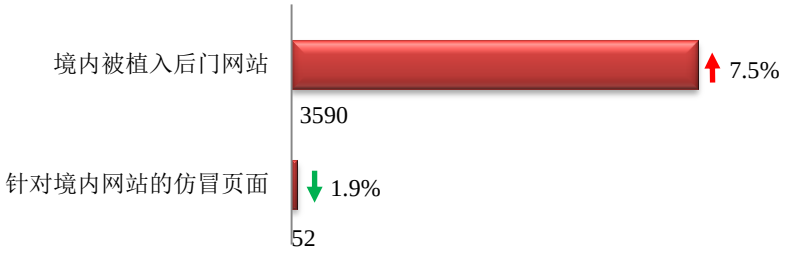
ANVA恶意地址黑名单发布地址

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。

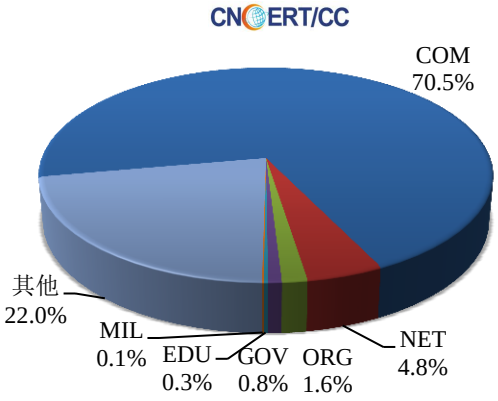
本周网站安全情况

本周 CNCERT 监测发现境内被植入后门的网站数量为 3590 个；针对境内网站的仿冒页面数量 52 个。



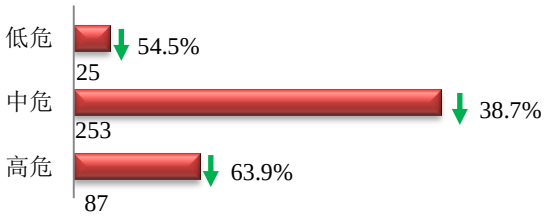
本周境内境内被植入后门的政府网站（GOV 类）数量为 30 个（约占境内 0.8%），较上周环比下降 9.1%；针对境内网站的仿冒页面涉及域名 30 个，IP 地址 25 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被植入后门网站按类型分布
(9/9-9/15)

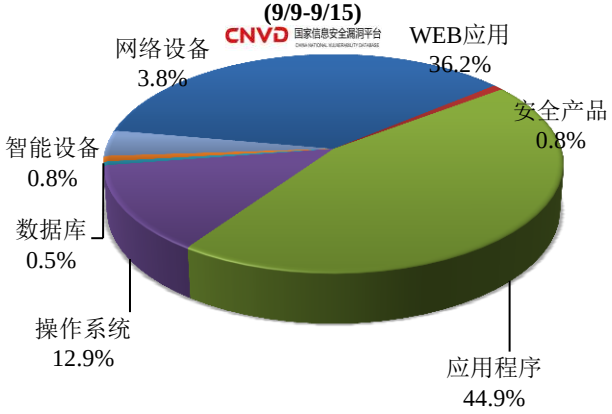


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 365 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
(9/9-9/15)



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。

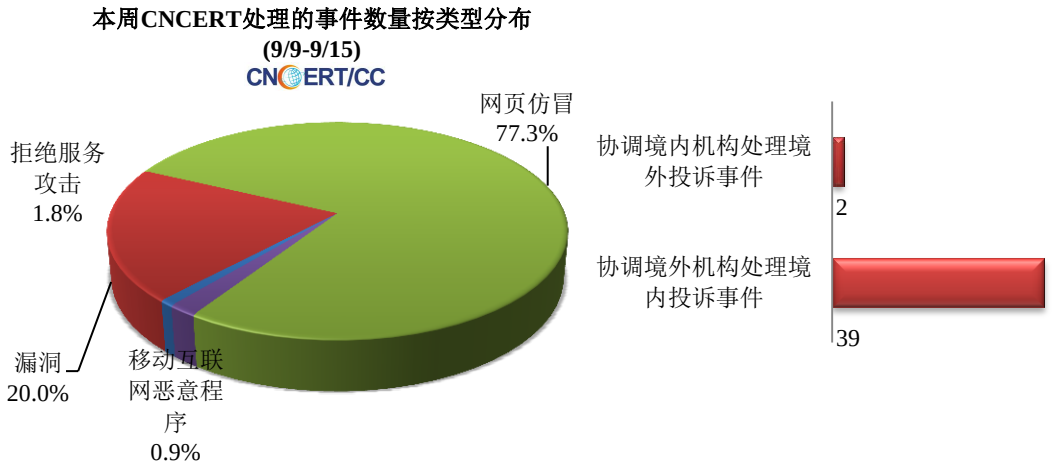
CNVD漏洞周报发布地址

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

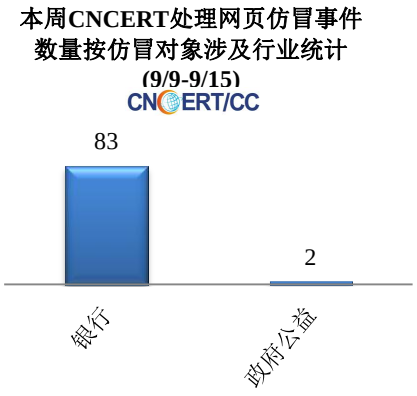
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

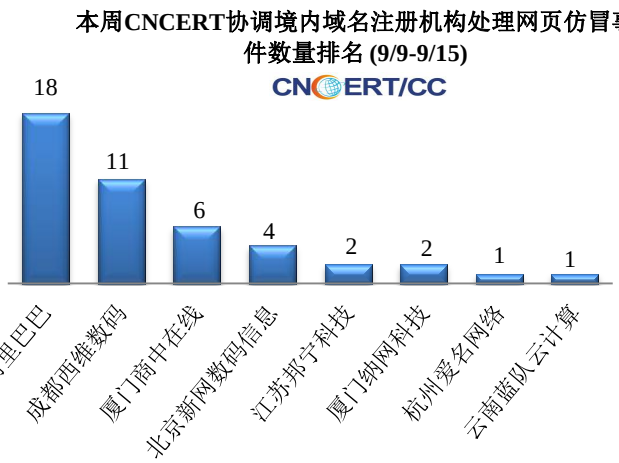
本周事件处理情况

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 110 起，其中跨境网络安全事件 41 起。



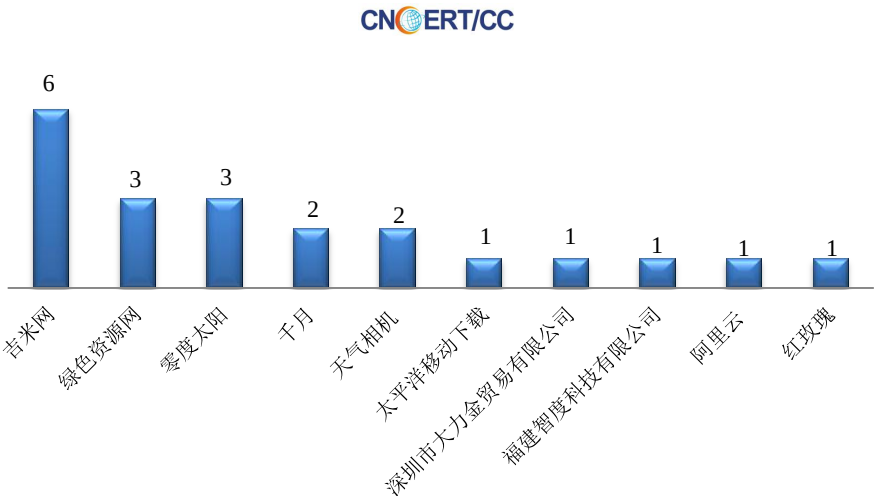
本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 85 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 83 起和其他事件 2 起。





本周，CNCERT 协调 10 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 21 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
(9/9-9/15)



业界新闻速递

1、 《网络生态治理规定（征求意见稿）》公开征求意见

9 月 10 日国家网信办消息，为了加强网络生态治理，维护良好网络秩序，保障公民、法人和其他组织的合法权益，构建天朗气清的网络空间，根据《中华人民共和国网络安全法》《互联网信息服务管理办法》《国务院关于授权国家互联网信息办公室负责互联网信息内容管理工作的通知》，国家互联网信息办公室会同有关部门起草了《网络生态治理规定(征求意见稿)》，向社会公开征求意见。

2、京津冀公共互联网网络安全应急演练顺利举行球

9 月 11 日，中国工信部消息，为有效提升协同应对重大网络安全突发事件的能力，做好国庆 70 周年网络安全保障工作，工信部网络安全管理局统一部署开展 2019 年度公共互联网网络安全应急演练。按照演练方案，天津市通信管理局会同北京市、河北省通信管理局于 9 月 5 日协同落实京津冀公共互联网网络安全应急演练，三地基础电信企业、重点互联网企业及中国信通院等单位参加，演练顺利举行。

3、贝索斯等 50 多位 CEO 签联名信 呼吁国会制定数据隐私法

9 月 10 日外媒 CNET 消息，包括亚马逊 CEO 杰夫·贝索斯（Jeff Bezos）在内的美国 50 多家大公司的 CEO 日前联名签署一封公开信，呼吁美国国会出台一项全面的消费者数据隐私法案。

签署联名信的这 51 位 CEO 表示，有必要制定一项联邦法律，以确保“对美国消费者进行有力、一致的保护”，并允许“美国公司继续领导一个具有全球竞争力的市场”。除了写给美国参众两院的领导人，这封信还写给众议院能源和商业委员会和参议院商业、科学和运输委员会的领导人。

4、黑客利用“Simjacker”漏洞窃取手机数据 或影响 10 亿人

9 月 14 日据 TNW 报道，网络安全研究人员警告称，SIM 卡存在一个被称为“Simjacker”的严重漏洞，使得远程攻击者可以在用户不知情的情况下发送短信攻击目标手机并监控受害者。据称，“Simjacker”漏洞攻击包括向手机发送一条短信，短信中包含一种特定类型的类似间谍软件的代码，然后手机会指示手机内的 SIM 卡控制手机，检索并执行敏感命令。这一漏洞存在于称为 S@T 的浏览器中，该浏览器作为 GSM 普遍使用的手机应用工具包(STK)的一部分，嵌入大多数手机 SIM 卡中，为客户提供增值服务。

AdaptiveMobile 表示，至少有 30 个国家的移动运营商积极使用 S@T 浏览器技术，总人数超过 10 亿。这就意味着，在全球或有逾 10 亿手机用户可能会受到影响。

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：王毓骏

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315