国家互联网应急中心

网络安全信息与动态周报

2020 年第 21 期

5 月 18 日-5 月 24 日

CNCERT/CC

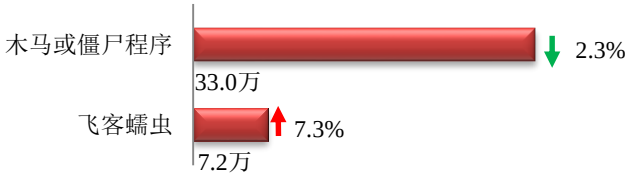
本周网络安全基本态势

境内感染网络病毒的主机数量	•40.2万	↓ 0.7%
境内被篡改网站总数 其中政府网站数量	•7698 •31	↑ 4.6% ↓ 24.4%
境内被植入后门网站总数 其中政府网站数量	•1798 •6	↑ 7.2% ↑ 100.0%
针对境内网站的仿冒页面数量	•476	↓ 42.4%
新增信息安全漏洞数量 其中高危漏洞数量	•289 •132	↓ 14.0% ↑ 14.8%

= 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

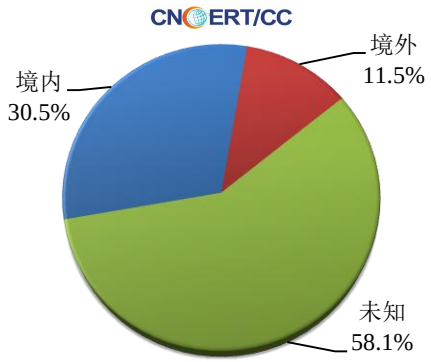
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 40.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 33.0 万以及境内感染飞客（conficker）蠕虫的主机约 7.2 万。

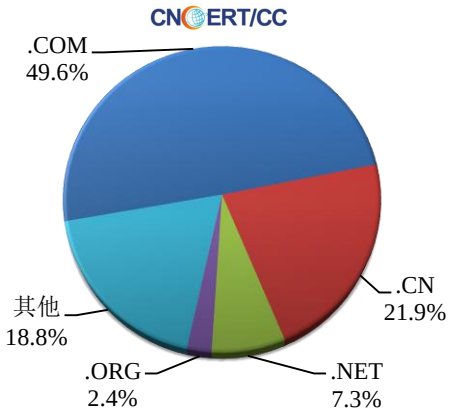


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 863 个，涉及 IP 地址 4040 个。在 863 个域名中，有 11.5%为境外注册，且顶级域为.com 的约占 49.6%；在 4040 个 IP 中，有约 59.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 335 个 IP。

本周放马站点域名注册所属境内外分布
(5/18-5/24)



本周放马站点域名所属顶级域的分布
(5/18-5/24)



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。

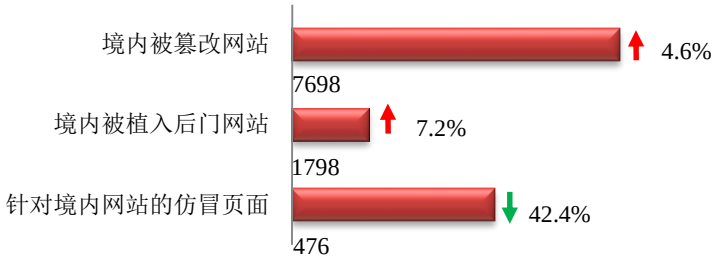
ANVA网络安全威胁信息共享平台

https://share.anva.org.cn/web/publicity/listurl

中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由 CNCERT 发起并组织运作的行业联盟。

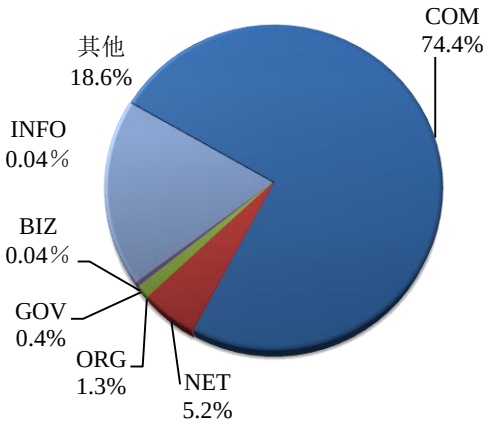
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 7698 个；被植入后门的网站数量为 1798 个；针对境内网站的仿冒页面数量 476 个。

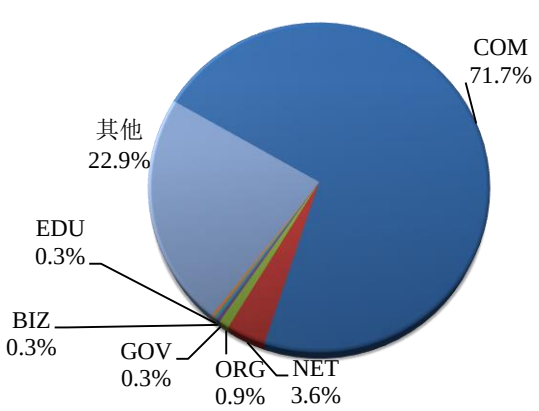


本周境内被篡改政府网站（GOV 类）数量为 31 个（约占境内 0.4%），较上周下降了 24.4%；境内被植入后门的政府网站（GOV 类）数量为 6 个（约占境内 0.3%），较上周上涨了 100.0%。

本周我国境内篡改网站按类型分布
(5/18-5/24)

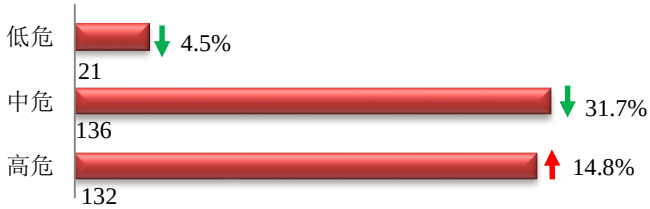


本周我国境内被植入后门网站按类型分类
(5/18-5/24)

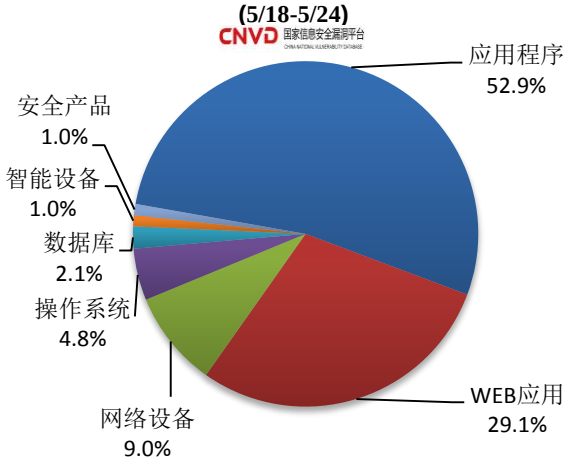


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 289 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分布
(5/18-5/24)



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 应用和网络设备。

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

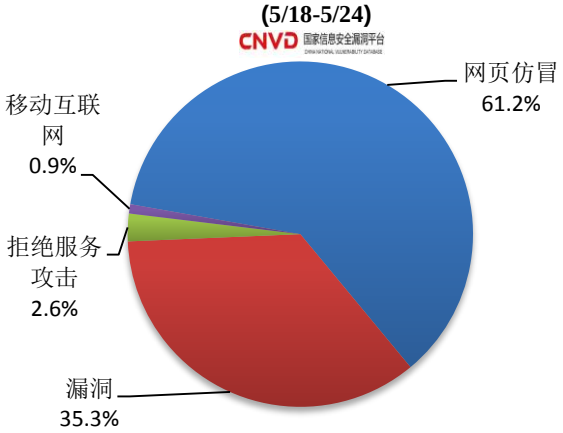
http://www.cnvd.org.cn/webinfo/list?type=4

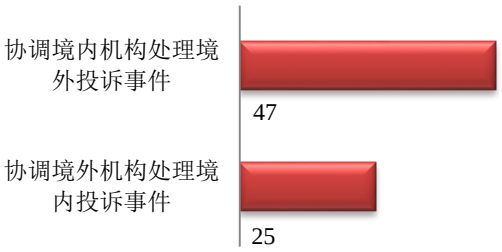
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

本周，CNCERT 协调基础电信企业、云服务商、域名注册服务机构、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 232 起，其中跨境网络安全事件 72 起。

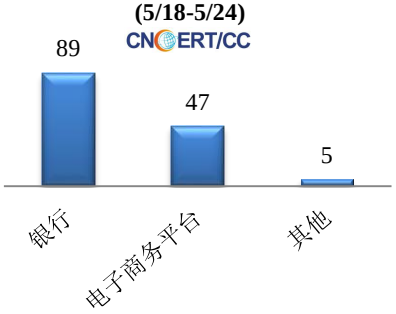
本周CNCERT处理的事件数量按类型分布 (5/18-5/24)



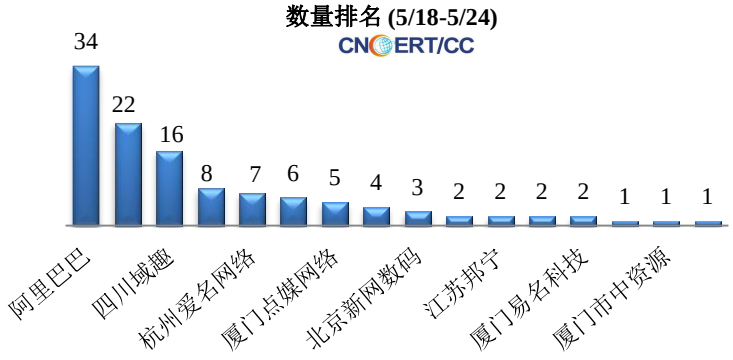


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 141 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 89 起、电子商务平台 47 起和其他事件 5 起。

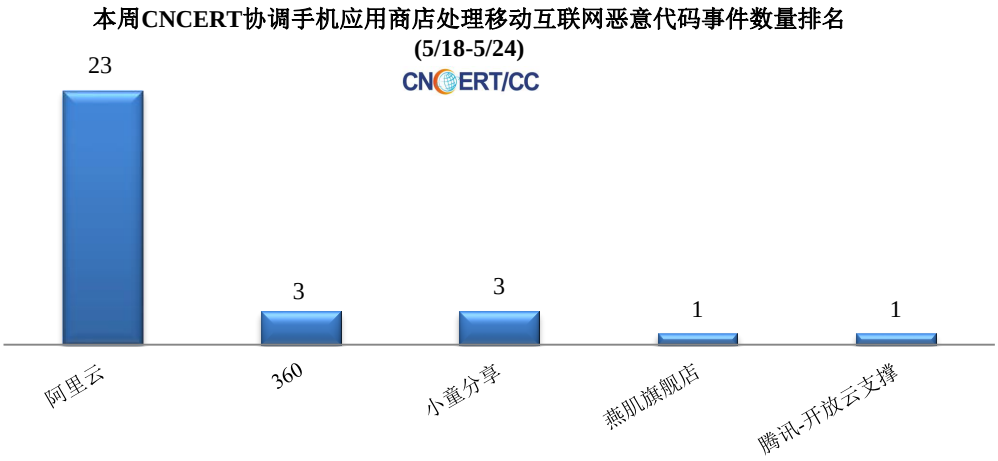
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (5/18-5/24)



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 (5/18-5/24)



本周，CNCERT 协调 5 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 31 个。



业界新闻速递

1、 国家网信办启动 2020“清朗”专项行动

5 月 22 日，据中国网信网消息，为进一步规范网上信息传播秩序，切实维护广大人民群众切身利益，促使网络空间更加清朗，即日起，国家网信办在全国范围内启动为期 8 个月的 2020“清朗”专项行动。

近年来，全国网信系统持续加大网络生态治理力度，深入整治网上各类违法违规问题乱象，舆论生态总体向好，网络治理成效明显。但色情低俗、网络暴力、恶意营销、侵犯公民个人隐私等负面有害信息花样不断翻新，极易反弹反复，严重污染网络生态环境，影响青少年身心健康，网民反映强烈、举报不断。为回应广大群众关切，国家网信办决定今年继续开展“清朗”专项行动。

国家网信办有关负责人介绍，“清朗”专项行动全面覆盖各类网络传播渠道和平台，集中清理网上各类违法和不良信息。专项行动将出重拳、用真招，对有令不行、顶风作案的网站平台依法从严处理，并公开曝光典型案例，有效震慑违法违规行为。

国家网信办有关负责人表示，“清朗”专项行动是网络综合治理的一项基础性、长期性任务，下一步将继续加大整治力度，建立完善长效治理机制，坚决遏制网上违法和不良信息蔓延态势。同时欢迎广大网民、媒体和社会各界积极参与，向网站平台和有关部门举报相关问题，携手共建清朗网络空间。

2、 Edison Mail 更新程序存在严重 BUG 同步后可随意访问他人账号内容

5 月 18 日，据 cnBeta 网站消息，Edison Mail 是一款在 iPhone、iPad 和 Mac 上比较

流行的第三方电子邮件应用，但近日曝光的一个 BUG 引起了网民对隐私的极大关注，有用户报告称，在该应用中开启新的账户同步功能后，他们可以完全访问其他 Edison Mail 用户的电子邮件账户。随后，Edison Mail 在对外发布一份声明，表示这个 BUG 目前只影响 iOS 用户，并只向少部分 iOS 用户推出了一个软件更新。在接到用户反馈后，厂商已经迅速回滚了该更新，并联系受影响的 Edison Mail 用户（仅限于过去 10 小时内更新并打开应用的用户子集）。并表示，目前来看，这似乎是一个 BUG，而不是安全漏洞。这个问题似乎源于上周在 Edison Mail 客户端推出的新同步功能。

3、 DNS 协议漏洞 NXNSAttack 可导致大型 DDoS 攻击

5 月 19 日，据 SECURITYWEEK 网站消息，以色列特拉维夫大学和以色列跨学科中心的一组研究人员发现新 DNS 漏洞，并称其为 NXNSAttack。该漏洞存在于 DNS 协议中，并且会影响所有递归 DNS 解析器，已被证实影响 NLnetLabs 的 Unbound、BIND、Knot Resolver 和 PowerDNS 等 DNS 软件，以及由谷歌、微软、Cloudflare、亚马逊、Oracle(DYN)、Verisign、IBM Quad9 和 ICANN 提供的 DNS 服务。受影响的供应商对该漏洞分别分配了 CVE 编号，包括 CVE-2020-8616(BIND)、CVE-2020-12662(Unbound)、CVE-2020-12667(Knot)、CVE-2020-10995(PowerDNS)。针对该漏洞，远程攻击者可以通过向易受攻击的解析器发送 DNS 查询来放大网络流量，该解析器会查询攻击者的权威服务器控制器。攻击者服务器将伪造的服务器名称委派给指向受害者 DNS 域的伪造服务器名，从而使解析程序生成对受害者的 DNS 服务器的查询，导致超过 1620 放大系数的 DDoS 攻击。

4、 蓝牙无线通信协议漏洞致无数设备易受 BIAS 攻击

5 月 19 日，据 welivesecurity 网站消息，研究人员在蓝牙无线通信协议（蓝牙 BR/EDR）中发现一个新漏洞，可能导致智能手机、笔记本电脑和智能家居等设备遭受“蓝牙模拟攻击”（BIAS）。研究人员对超 28 种产品蓝牙芯片进行了 BIAS 攻击测试，包括赛普拉斯、高通、苹果、英特尔、三星和 CSR 等，均发现容易遭受 BIAS 攻击。研究人员表示 BIAS 攻击是第一类成功绕过蓝牙认证过程的攻击，该过程发生在建立安全连接的过程中。攻击中利用的漏洞包括缺乏完整性保护、加密和相互身份验证。利用该漏洞，攻击者可以假冒经过身份验证过程并与另一台设备配对的其中一台设备，进而可能远程控制设备并从中窃取数据。

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 2019 年，CNCERT 已与 78 个国家和地区的 260 个组织建立了“CNCERT 国际合作伙伴”关系。CNCERT 还积极参加亚太经合组织、国际电联、上合组织、东盟、金砖等政府层面国际和区域组织的网络安全相关工作。

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：吕卓航

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315