国家互联网应急中心

网络安全信息与动态周报

2020 年第 18 期

4 月 27 日-5 月 3 日

CNCERT/CC

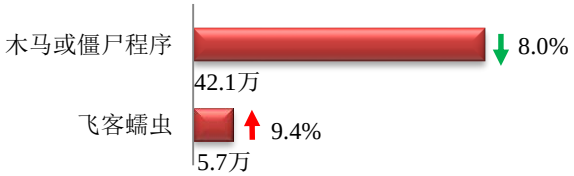
本周网络安全基本态势

境内感染网络病毒的主机数量2	•47.8万	↓ 6.2%
境内被篡改网站总数 其中政府网站数量	•7269 •37	↑ 70.4% ↑ 60.9%
境内被植入后门网站总数 其中政府网站数量	•1845 •4	↑ 62.1% ↑ 300.0%
针对境内网站的仿冒页面数量	•278	↑ 22.5%
新增信息安全漏洞数量 其中高危漏洞数量	•374 •160	↓ 29.8% ↓ 36.8%

= 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

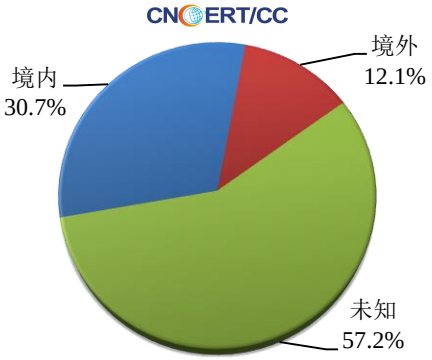
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 47.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 42.1 万以及境内感染飞客（conficker）蠕虫的主机约 5.7 万。

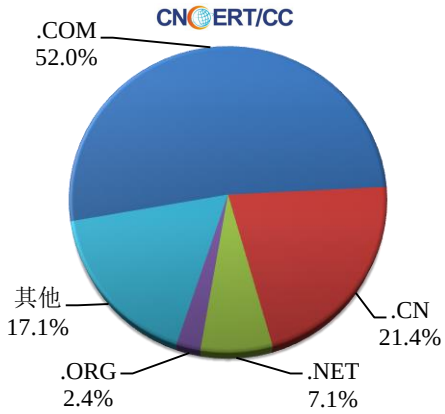


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 1168 个，涉及 IP 地址 5232 个。在 1168 个域名中，有 12.1%为境外注册，且顶级域为.com 的约占 53.3%；在 5232 个 IP 中，有约 53.0%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 592 个 IP。

本周放马站点域名注册所属境内外分布
(4/27-5/3)



本周放马站点域名所属顶级域的分布
(4/27-5/3)



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。

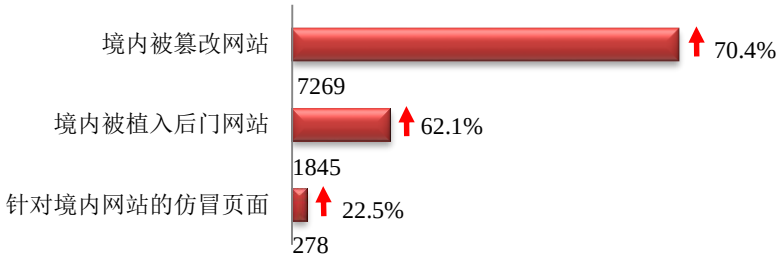
ANVA恶意地址黑名单发布地址

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。

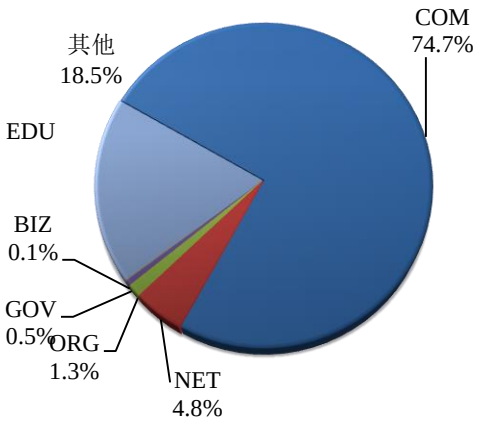
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 7269 个；被植入后门的网站数量为 1845 个；针对境内网站的仿冒页面数量 278 个。

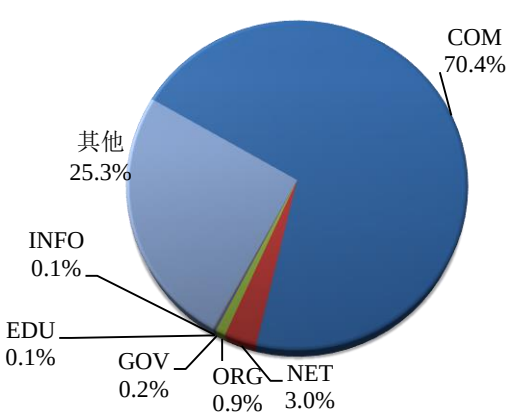


本周境内被篡改政府网站（GOV 类）数量为 37 个（约占境内 0.5%），较上周上涨了 60.9%；境内被植入后门的政府网站（GOV 类）数量为 4 个（约占境内 0.2%），较上周上涨了 300.0%。

本周我国境内篡改网站按类型分布
(4/27-5/3)

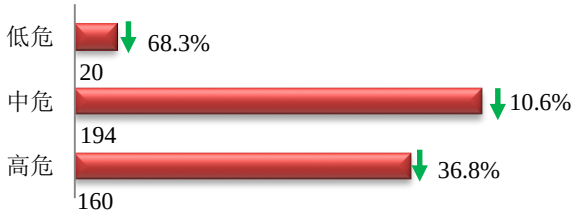


本周我国境内被植入后门网站按类型分类
(4/27-5/3)

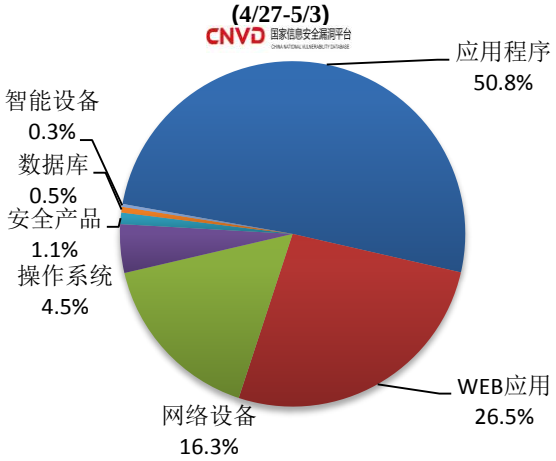


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 374 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
(4/27-5/3)



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

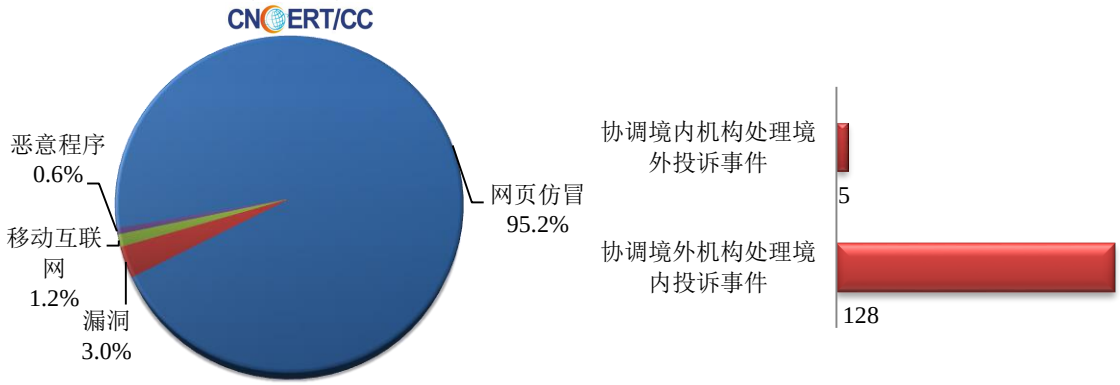
http://www.cnvd.org.cn/webinfo/list?type=4

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

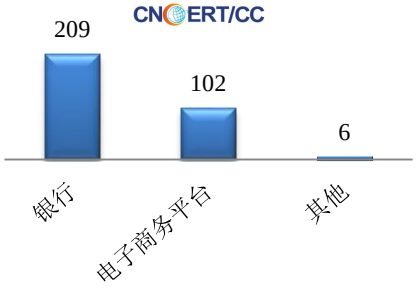
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 333 起，其中跨境网络安全事件 133 起。

本周CNCERT 处理的事件数量按类型分布
(4/27-5/3)

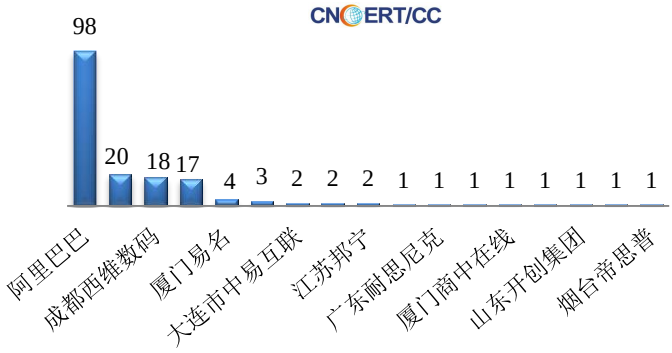


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 317 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 209 起、电子商务平台 102 起和其他仿冒事件 6 起。

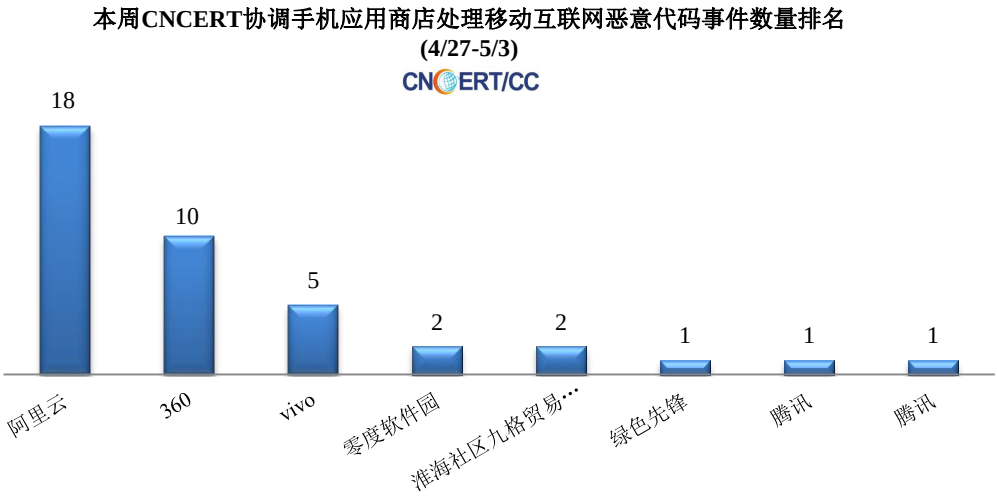
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计
(4/27-5/3)



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 (4/27-5/3)



本周，CNCERT 协调 8 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 40 个。



业界新闻速递

1、 网信办等 12 部门联合发布《网络安全审查办法》

为了确保关键信息基础设施供应链安全，维护国家安全，国家互联网信息办公室、发展改革委、工信部等 12 部门 4 月 27 日联合发布《网络安全审查办法》。《办法》将于今年 6 月 1 日起实施。

根据《办法》，网络安全审查重点评估采购网络产品和服务可能带来的国家安全风险，包括产品和服务使用后带来的关键信息基础设施被非法控制、遭受干扰或破坏，以及重要数据被窃取、泄露、毁损的风险；产品和服务的安全性、开放性、透明性、来源的多样性，供应渠道的可靠性以及因为政治、外交、贸易等因素导致供应中断的风险；以及其他可能危害关键信息基础设施安全和国家安全的因素等。《办法》还指出，电信、广播电视、能源、金融、公路水路运输、铁路、民航等行业领域的重要网络和信息系统运营者在采购网络产品和服务时，应当按照要求考虑申报网络安全审查。

2、 英国成立在线安全技术行业协会

4 月 27 日，据外媒报道，在英国政府、活动人士和慈善机构的支持下，英国 14 家科技公司成立了“在线安全技术行业协会”（Online Safety Tech Industry Association），旨在解决在线安全问题。该行业协会由爱丁堡安全公司 Cyan Forensics 和公共部门创业机构 body public 运营，最初在 2019 年探讨网络危害的圆桌会议上被构想出来。它有三个核心目标：通过向政策制定者、技术提供商和广泛公众提供有关在线安全技术的信息，

发出“希望之声”；创造并利用其在政策、监管和更广泛的行业支持方面的集体影响力；为在线安全专家提供讨论平台。

3、 美国 NIST 发布白皮书，以提高服务器平台安全性和数据保密性

4 月 28 日，美国国家标准与技术研究院（NIST）发布《为服务器平台启用硬件安全性：为云计算和边缘计算用例启用平台安全的分层方法（草案）》白皮书。白皮书解释了基于硬件的安全技术，并举例说明可以提高云数据中心和边缘计算平台安全性和数据保密性的技术，旨在推广以物理平台为底层安全框架的统一安全控制。白皮书围绕硬件安全模块、信任链和大量因特尔（Intel）旗下的技术标准开展用例分享。全书包含“硬件平台安全概述、平台完整性验证、数据保护和保密计算、远程认证服务、利用基于硬件的安全性的云用例场景、未来演进方向”六个方面。

英国 14 家科技公司成立“在线安全技术行业协会”

4、 法国费加罗报数据库泄露 74 亿条记录

5 月 2 日，据外媒报道，Security Detectives 的安全研究人员发现法国发行量最大综合性日报费加罗报(Le Figaro)出现数据泄露事件。泄露的数据量超过 8TB，涉及 74 亿条记录，包括费加罗报网站注册用户的登陆凭证。泄露的个人身份信息包括邮箱、全名、家庭地址、口令、居住地和邮编、IP 地址、外部服务器访问 token。此外，泄露的数据库中也含有大量关于费加罗报服务器的技术日志信息，这些敏感数据对黑客入侵企业的数据基础设施是非常有价值的。包括 SQL 查询错误、不同服务器之间的流量、通信协议、对 admin 账户的潜在访问。许多泄露的信息都指向一个 AGORA 系统，可能是该公司使用的 CRM 系统。安全研究人员发现该数据库是没有密码保护的，直接暴露在公网上。任何人只要有数据库的 IP 地址就可以访问。

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：周昊

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315