国家互联网应急中心

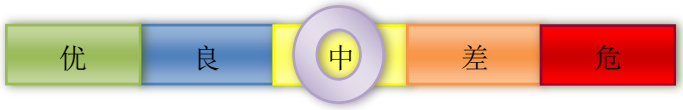
网络安全信息与动态周报

2020 年第 13 期

3 月 23 日-3 月 29 日

CNCERT/CC

本周网络安全基本态势

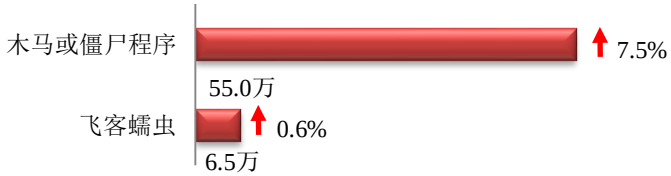


境内感染网络病毒的主机数量	•61.5万	↑6.7%
境内被篡改网站总数 其中政府网站数量	•7555 •22	↓22.6% ↓31.3%
境内被植入后门网站总数 其中政府网站数量	•1644 •9	↓5.1%
针对境内网站的仿冒页面数量	•852	↓48.8%
新增信息安全漏洞数量 其中高危漏洞数量	•504 •215	↑38.1% ↑108.7%

= 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

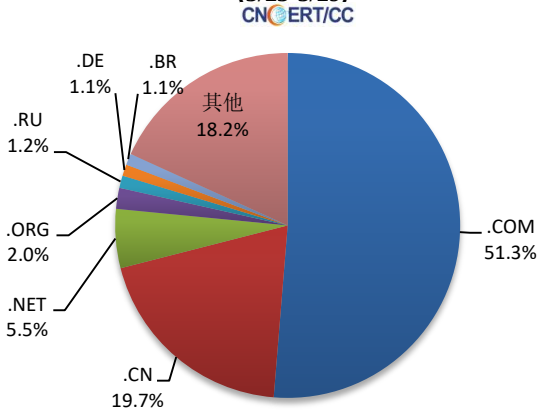
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 61.5 万个，其中包括境内被木马或被僵尸程序控制的主机约 55.0 万以及境内感染飞客（conficker）蠕虫的主机约 6.5 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 1121 个，涉及 IP 地址 4323 个。在 1121 个域名中，顶级域为.com 的约占 51.3%；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 355 个 IP。

本周放马站点域名所属顶级域的分布
(3/23-3/29)



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。

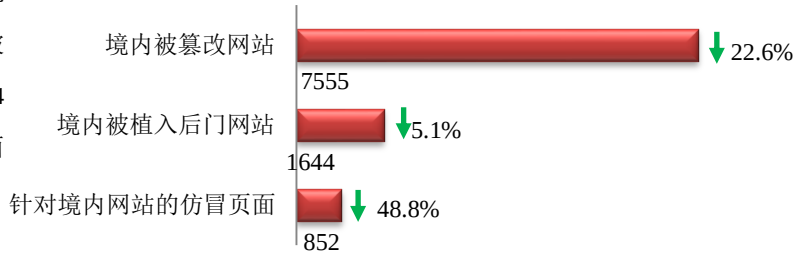
ANVA恶意地址黑名单发布地址

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。

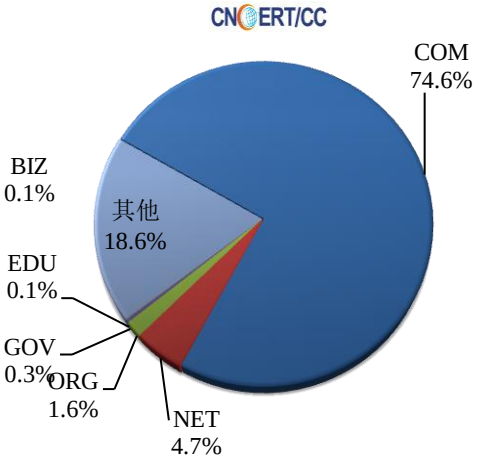
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 7555 个；被植入后门的网站数量为 1644 个；针对境内网站的仿冒页面数量 852 个。

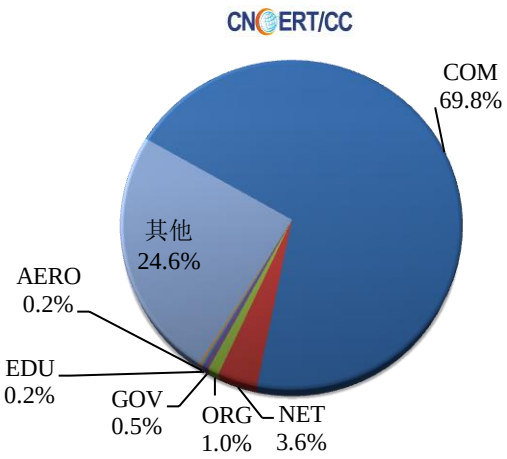


本周境内被篡改政府网站（GOV 类）数量为 22 个（约占境内 0.3%），较上周下降了 31.3%；境内被植入后门的政府网站（GOV 类）数量为 9 个（约占境内 0.5%）。

本周我国境内篡改网站按类型分布
(3/23-3/29)

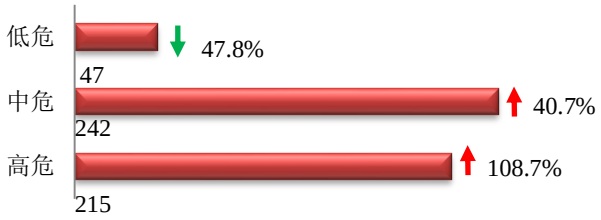


本周我国境内被植入后门网站按类型分类
(3/23-3/29)

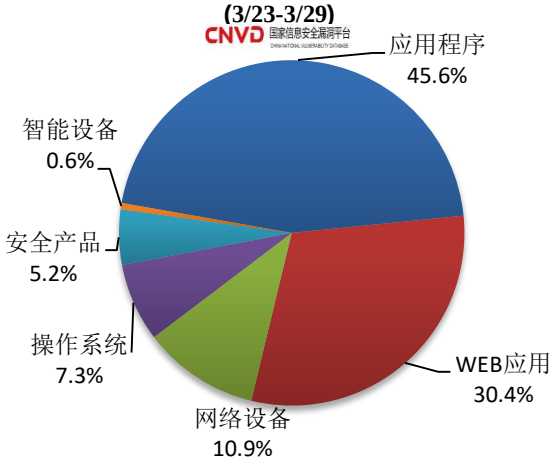


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 504 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
(3/23-3/29)



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

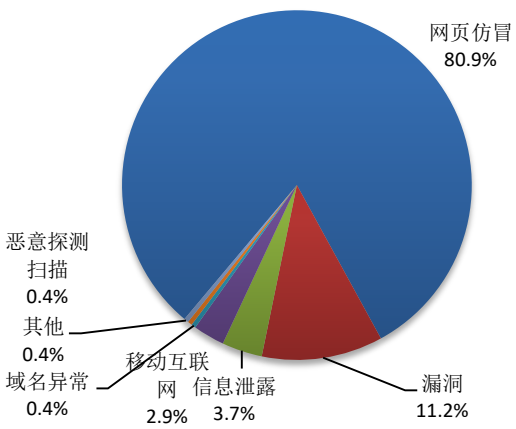
http://www.cnvd.org.cn/webinfo/list?type=4

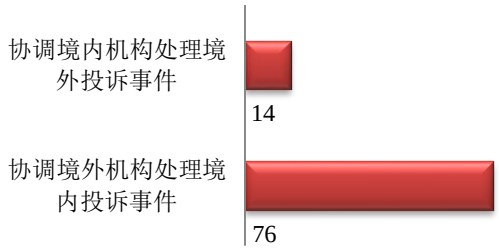
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 241 起，其中跨境网络安全事件 90 起。

本周CNCERT处理的事件数量按类型分布 (3/23-3/29)



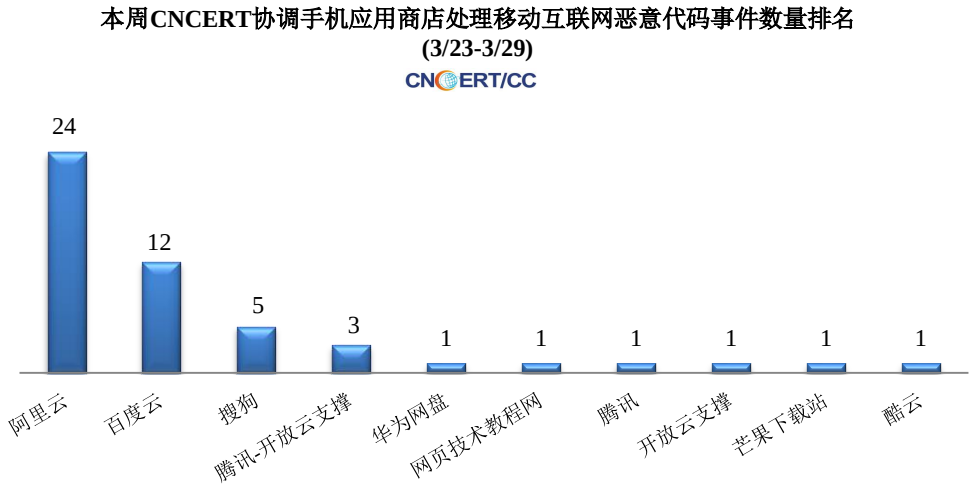


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 195 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包括银行仿冒事件 162 起和电子商务平台 16 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (3/23-3/29)

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 (3/23-3/29)

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 50 个。



业界新闻速递

1、 工信部：强化 5G 网络数据安全保护培育 5G 网络安全生态

3 月 24 日，为深入贯彻落实习近平总书记关于推动 5G 网络加快发展的重要讲话精神，全力推进 5G 网络建设、应用推广、技术发展和安全保障，充分发挥 5G 新型基础设施的规模效应和带动作用，支撑经济高质量发展，工业和信息化部发布了关于推动 5G 加快发展的通知。通知包括五大方面内容：进一步加快 5G 网络建设部署、丰富 5G 技术应用场景、持续加大 5G 技术研发力度、着力构建 5G 安全保障体系、加强组织实施。

2、 特朗普政府签署最新 5G 安全法案 将和盟国共同推进战略政策

3 月 25 日，据外媒报道，近日白宫发布了 5G 安全战略政策文件，列出了特朗普政府改善 5G 无线网络安全的广泛政策重点，其中包括与盟国合作以实现这一目标的承诺。据悉，文件中明确指出，5G 将成为美国繁荣的主要驱动力，一旦政府拥有非常快的网络连接能力，未来数百亿个新项目将具有无限可能，因此部署和建设安全可靠的 5G 通信基础设施对于保障 5G 安全是至关重要的。该战略表明了特朗普政府旨在“与最亲密的合作伙伴武装起来”共同领导 5G 发展的趋势。与此同时，特朗普总统于上周早些时候签署了两项无线法案，一项旨在制定 5G 网络安全计划，另一项旨在确保宽带数据图的准确性。

3、 有关新冠病毒网络攻击激增 世卫组织成黑客目标

3 月 23 日，据路透社报道，3 月早些时候，黑客试图入侵世界卫生组织。虽然没有

成功入侵，但该机构表示，随着他们努力遏制新冠病毒，网络攻击增加了两倍多。网络安全专家向路透社通报了这起试图入侵世卫组织的事件，并追踪可疑的互联网域名注册活动。该专家表示，其在 3 月 13 日左右发现这一活动的，当时他跟踪的一群黑客启动了一个恶意网站，模仿世界卫生组织的内部电子邮件系统。

4、 黑客劫持路由器 DNS：以 COVID-19 之名重定向至恶意网站

3 月 27 日，据 cnbeta 网站报道，安全公司 Bitdefender 研究人员 26 日发布博文，发现了通过 DNS 劫持将用户重定向到新冠病毒（COVID-19）信息 App 的下载页面。用户访问页面之后并不会下载任何 App 文件，会直接被恶意程序感染，并会获取诸如加密钱包凭证和其他私人敏感信息。研究人员表示，黑客向存在漏洞的路由器发起攻击，并使用暴力破解的方式来猜测控制面板的密码。一旦攻击成功，黑客便会更改路由器的 DNS 设置，将一些域名指向自己的服务器。研究人员认为，大约有 1200 人受到此攻击的影响，并且该团队到目前为止已找到四个单独的恶意 Bitbucket 存储库。从地理上来讲，大多数受害者似乎来自美国，德国和法国。

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 与 76 个国家和地区的 233 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：韩志辉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315