国家互联网应急中心

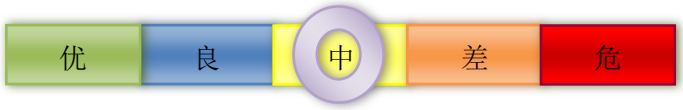
网络安全信息与动态周报

2020 年第 12 期

3 月 16 日-3 月 22 日

CNCERT/CC

本周网络安全基本态势

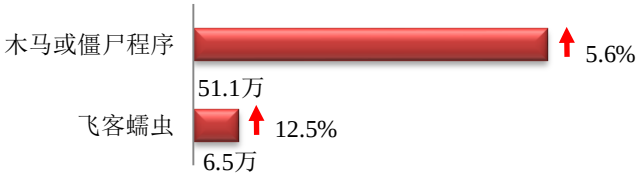


境内感染网络病毒的主机数量	•57.6万	↑6.3%
境内被篡改网站总数 其中政府网站数量	•9756 •32	↑21.3% ↑14.3%
境内被植入后门网站总数 其中政府网站数量	•1732 •0	↑17.8% ↓100.0%
针对境内网站的仿冒页面数量	•1665	↑73.1%
新增信息安全漏洞数量 其中高危漏洞数量	•365 •103	↓12.5% ↓25.4%

= 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

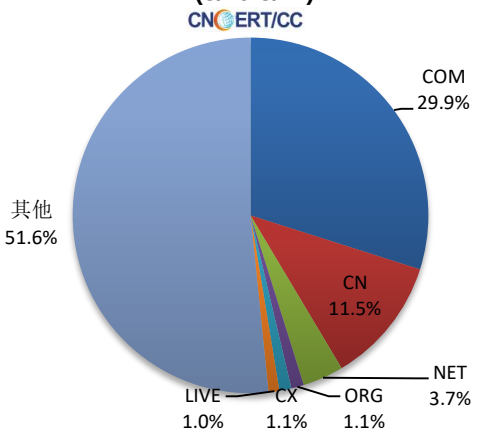
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 57.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 51.1 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 1829 个，涉及 IP 地址 4718 个。在 1829 个域名中，顶级域为.com 的约占 29.9%；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 362 个 IP。

本周放马站点域名所属顶级域的分布
(3/16-3/22)



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。

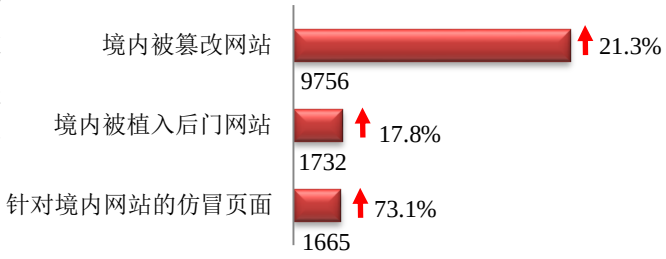
ANVA恶意地址黑名单发布地址

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。

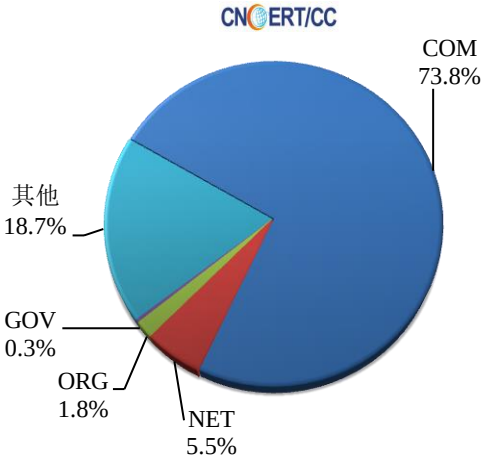
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 9756 个；被植入后门的网站数量为 1732 个；针对境内网站的仿冒页面数量 1665 个。

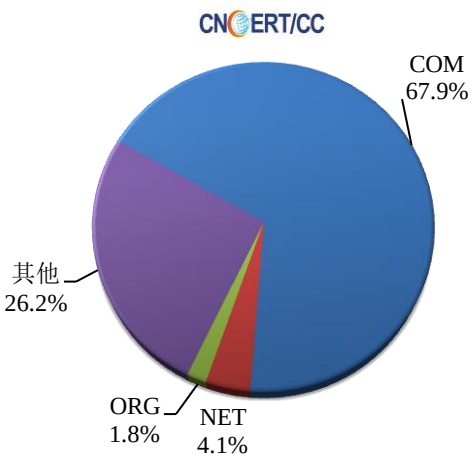


本周境内被篡改政府网站（GOV 类）数量为 32 个（约占境内 0.3%），较上周上涨了 14.3%；境内被植入后门的政府网站（GOV 类）数量为 0 个（约占境内 0.0%），较上周下降了 100.0%。

本周我国境内篡改网站按类型分布
(3/16-3/22)

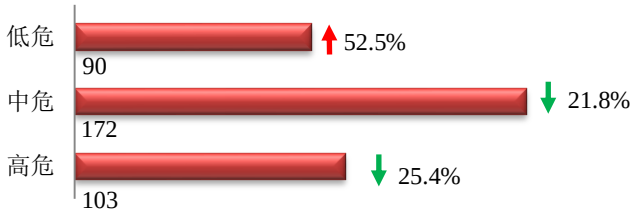


本周我国境内被植入后门网站按类型分类
(3/16-3/22)

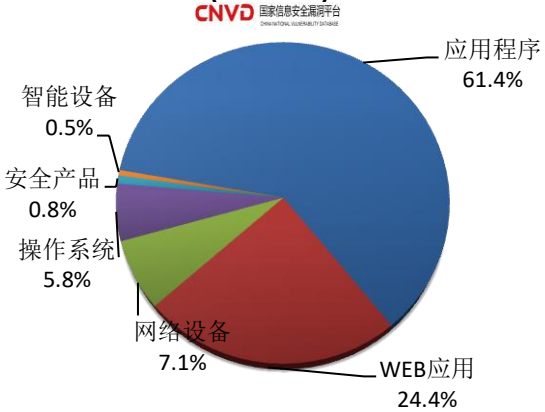


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 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分布
(3/16-3/22)



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

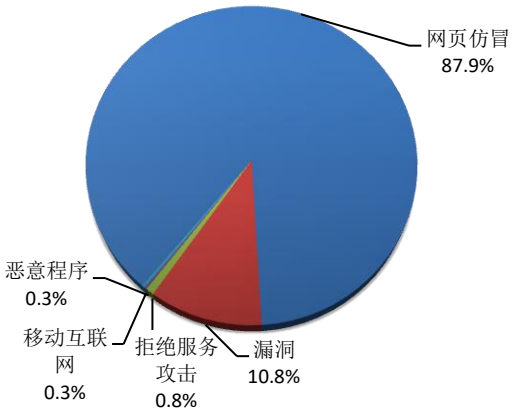
http://www.cnvd.org.cn/webinfo/list?type=4

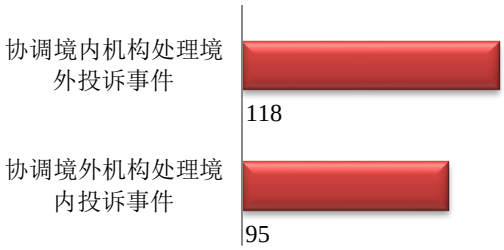
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 390 起，其中跨境网络安全事件 213 起。

本周CNCERT处理的事件数量按类型分布 (3/16-3/22)



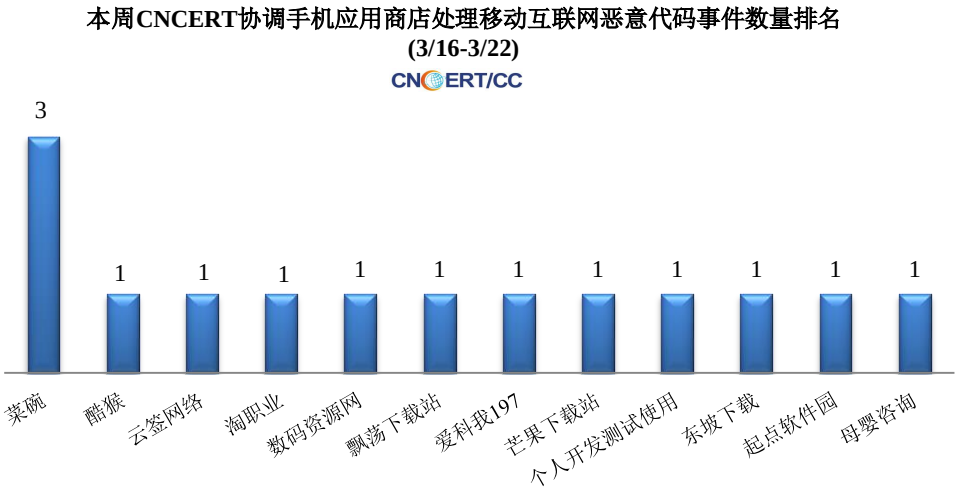


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 343 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包括银行仿冒事件 210 起和电子商务平台 118 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (3/16-3/22)

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 (3/16-3/22)

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 14 个。



业界新闻速递

1、 信安标委公开征集《网络安全标准实践指南—移动互联网应用程序收集使用个人信息自评估指南》意见

3 月 19 日，为落实《网络安全法》相关要求，围绕中央网信办、工信部、公安部、市场监管总局联合制定的《App 违法违规收集使用个人信息行为认定方法》，并基于 App 专项治理工作组发布的《App 违法违规收集使用个人信息自评估指南》，全国信息安全标准化技术委员会秘书处组织编制了《网络安全标准实践指南—移动互联网应用程序（App）收集使用个人信息自评估指南（征求意见稿）》。

根据《全国信息安全标准化技术委员会<网络安全标准实践指南>管理办法（暂行）》要求，全国信息安全标准化技术委员会秘书处组织对《网络安全标准实践指南—移动互联网应用程序（App）收集使用个人信息自评估指南（征求意见稿）》面向社会公开征求意见。

2、 欧委会通过欧盟 5G 安全工具箱

3 月 17 日，“C114”网站消息，欧委会通过应对 5G 网络安全风险的工具箱。该工具箱包括战略和技术措施，解决包括非技术因素风险在内的所有已评估出的风险。各成员国同意加强安全要求，评估供应商的风险状况，对被认为是高风险的供应商施加相关限制,包括对如核心网络功能等关键和敏感的资产进行排除等，制定确保供应商多元化的策略。虽然对具体安全措施的决定仍然是成员国的权责，但是该工具箱表明了欧盟各国

共同应对 5G 网络安全性挑战的坚定决心。欧委会将支持实施关于 5G 网络安全的欧盟方法，并将根据成员国的要求，酌情使用所有可用工具，以确保 5G 基础架构和供应链的安全性，包括：电信和网络安全规则；协调标准化以及欧盟范围内的认证；审查外国直接投资，保护欧洲 5G 供应链；贸易防御工具；竞争法；确保公共采购适当考虑安全方面；确保欧盟资助项目的受益人符合相关的安全要求。欧委会呼吁成员国采取行动，在 2020 年 4 月 30 日前落实工具箱建议的系列措施，并在 2020 年 6 月 30 日前就每个成员国的执行情况编写一份联合报告。

3、 捷克最大冠状病毒研究实验室遭神秘网络攻击

3 月 17 日，“E 安全”网站消息，捷克最大的新型冠状病毒测试实验室站点布尔诺大学医院遭到神秘网络攻击，目前该袭击正在中欧相关国家横行。此次攻击被认为严重到足以推迟紧急外科手术，外部推测该实验室的医疗系统遭到严重破坏。事件发生后，捷克国家网络安全中心、捷克警察和医院的 IT 人员组成了安全团队在现场合作，以恢复医院的 IT 网络。根据专家研究，冠状病毒在捷克可能刚开始传播，在这最危急的时刻，黑客似乎看到了发动勒索软件攻击的机会。

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：吕志泉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315