国家互联网应急中心

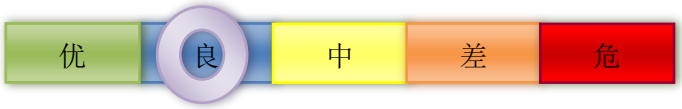
2019 年第 9 期

2 月 25 日-3 月 3 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

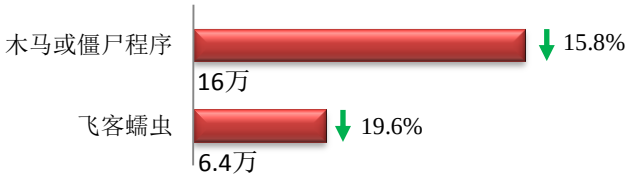


境内感染网络病毒的主机数量	•22.4万	↓16.9%
境内被篡改网站总数 其中政府网站数量	•600 •31	↑3.4% ↓29.5%
境内被植入后门网站总数 其中政府网站数量	•510 •8	↑14.6% ↓27.3%
针对境内网站的仿冒页面数量	•1518	↑7.2%
新增信息安全漏洞数量 其中高危漏洞数量	•379 •152	↑95.4% ↑216.7%

=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

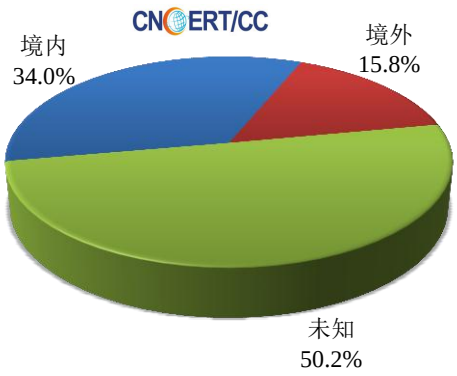
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 22.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 16.0 万以及境内感染飞客（conficker）蠕虫的主机约 6.4 万。

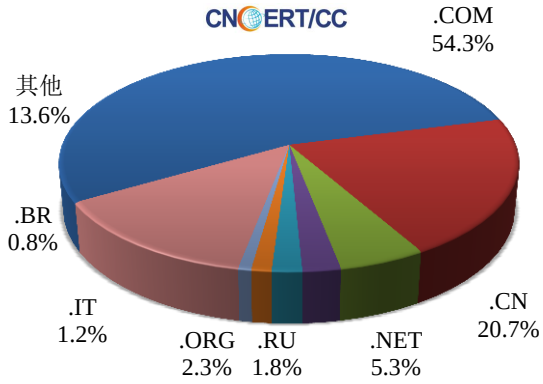


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 3303 个，涉及 IP 地址 7809 个。在 3303 个域名中，有 15.8%为境外注册，且顶级域为.com 的约占 54.3%；在 7809 个 IP 中，有约 60.9%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 697 个 IP。

本周放马站点域名注册所属境内外分布
(2/25-3/3)



本周放马站点域名所属顶级域的分布
(2/25-3/3)



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。

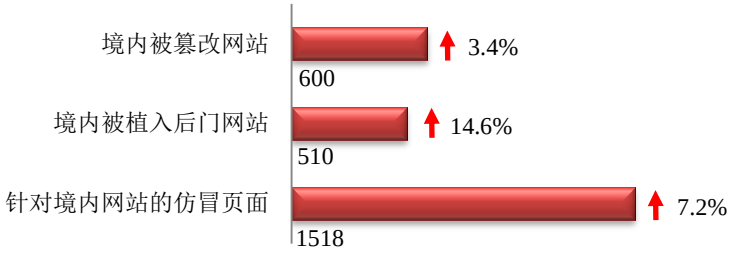
ANVA恶意地址黑名单发布地址

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。

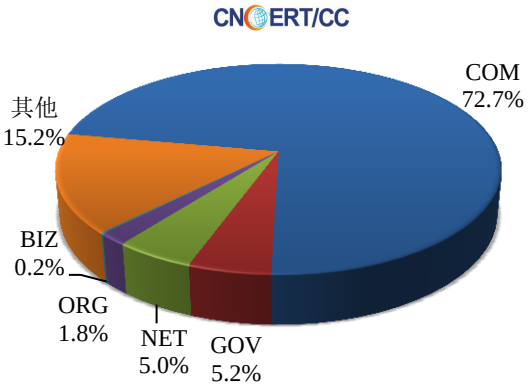
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 600 个；境内被植入后门的网站数量为 510 个；针对境内网站的仿冒页面数量 1518 个。

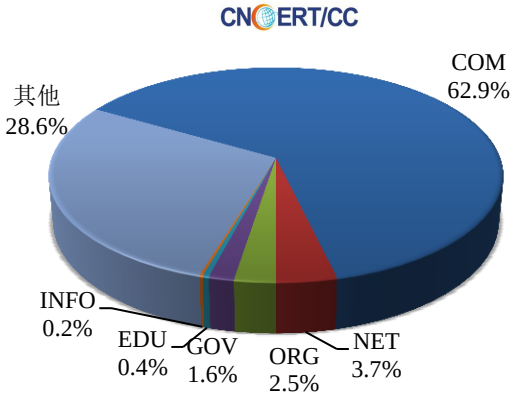


本周境内被篡改政府网站（GOV 类）数量为 31 个（约占境内 5.2%），较上周环比下降了 29.5%；境内被植入后门的政府网站（GOV 类）数量为 8 个（约占境内 1.6%），较上周环比下降了 27.3%%；针对境内网站的仿冒页面涉及域名 462 个，IP 地址 244 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(2/25-3/3)

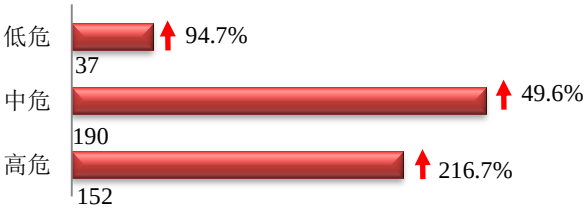


本周我国境内被植入后门网站按类型分布
(2/25-3/3)

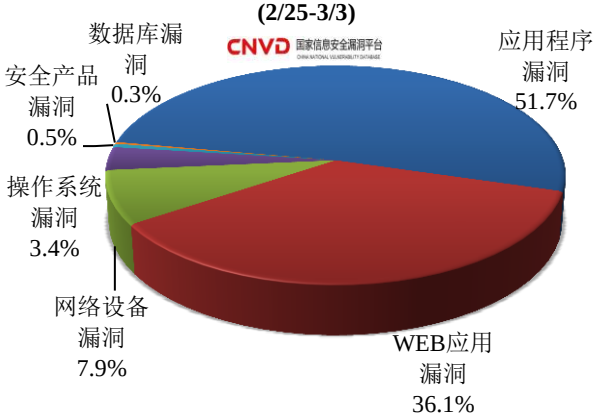


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 379 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
(2/25-3/3)



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 应用漏洞和网络设备漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

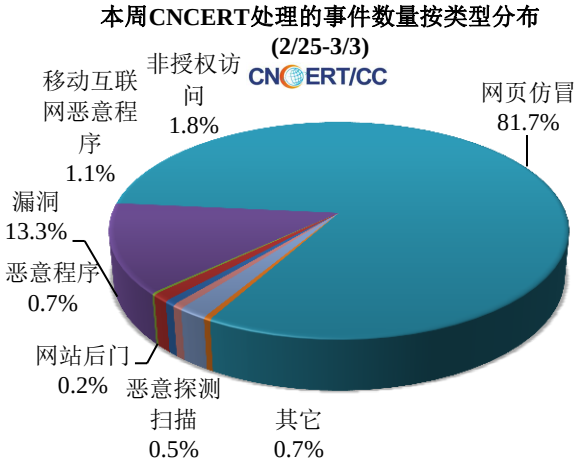
CNVD漏洞周报发布地址

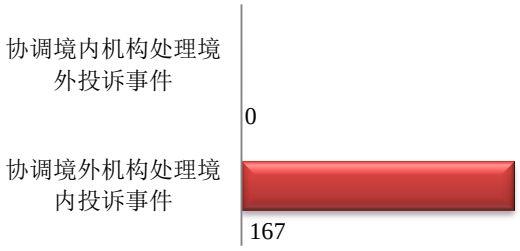
http://www.cnvd.org.cn/webinfo/list?type=4

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。

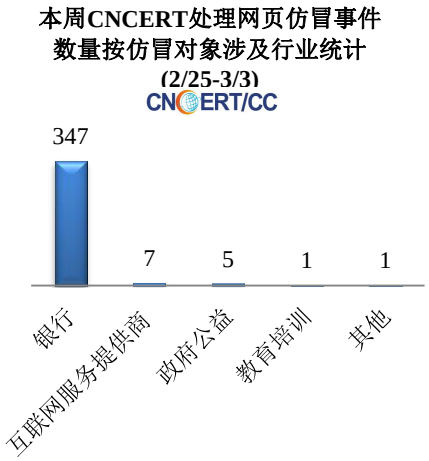
本周事件处理情况

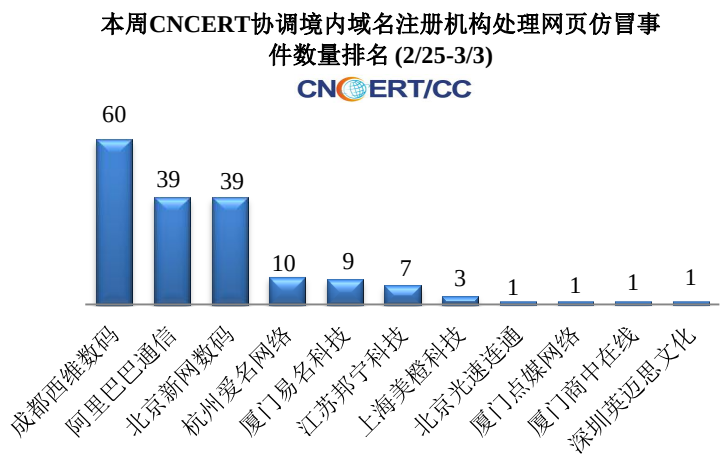
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 442 起，其中跨境网络安全事件 167 起。



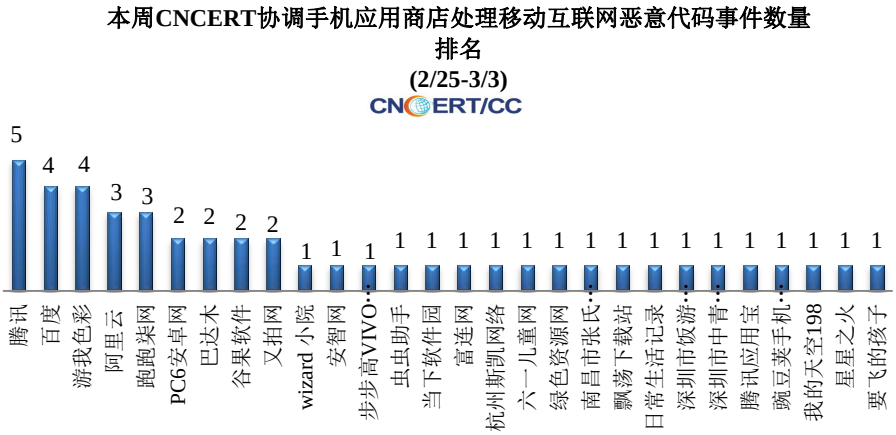


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 361 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 347 起和互联网服务提供商冒事件 7 起。





本周，CNCERT 协调 28 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 46 个。



业界新闻速递

1、美司法部发布《美国司法部数据战略》

安全内参 2 月 28 日消息 美司法部近日发布《美国司法部数据战略》，通过建立通用的方法、工具和流程对整个组织的数据进行管理和共享。为了最大限度发挥数据资产的价值，建立可持续的数据文化，该战略明确了四项基本目标，分别为：数据管理。开发数据生命周期所需的架构、政策和流程，并严格执行；数据共享。鼓励在司法部进行数据共享； 身份、凭据和访问管理。提供安全、及时、高效的关键任务信息访问能力； 数据劳动力培养。通过员工培训等方式，建立可持续的数据劳动力文化。

2、澳大利亚通过《援助和准入法案》，将削减加密通信安全

安全内参 3 月 2 日消息 澳大利亚议会通过了《援助与访问法案》(Assistance and Access Bill)，允许澳大利亚的情报机构和执法部门访问端到端的加密通信。许多美国科技巨头认为这是一项“反加密”法律，即便是专门为执法部门设计的后门，也有可能被坏人利用。当单独设备被黑客攻击时，其背后的互联网基础设施大门也随之打开，这将从根本上削弱澳大利亚的网络安全。

3、泰国通过网络安全法案

cnBeta.COM3 月 1 日消息 泰国政府通过了一项备受争议的网络安全法案，该法案因模糊不清以及能够全面访问互联网用户数据而受到批评。该法案在去年年底因对潜在数据访问受到批评后进行了修订，但该法案在泰国议会以 133 票赞成票、16 票弃权票获通过。泰国民众担心法律会被政府“武器化”，以使批评者沉默。在被视为国家紧急事件的案件中搜查和扣押数据和设备。这可以在没有法院命令的情况下实现互联网流量监控和访问私人数据，包括通信。

4、马耳他银行恐又遭黑客攻击

E 安全 3 月 2 日消息 马耳他最大的金融机构之一——瓦莱塔银行（Bank of Valletta，BOV）于 2 月 26 日暂时关闭了服务。瓦莱塔银行 2 月 26 日在其网站上发表声明称，瓦莱塔银行的互联网连接出现了问题，主要影响与互联网银行、移动银行以及通过 EPOS 机和网站进行银行卡支付相关的服务。银行正在努力解决这些技术问题。政府开始处理在瓦莱塔银行网络上检测到的网络入侵后，ATM、互联网和移动银行、销售点系统以及内部电子邮件停止了服务。

美国 2018 年中期选举当天，俄罗斯“巨魔工厂”的网络被切断！

5、道琼斯公司 240 万高风险客户的观察名单已遭泄露

新浪科技 2 月 28 日消息 据报道，在有权访问数据库的公司将其留在没有密码的服务器上之后，道琼斯所拥有的风险个人和公司实体的观察名单已被泄露。独立安全研究员发现亚马逊网络服务托管的 Elasticsearch 数据库暴露了 240 多万个人或商业实体的记录。这些数据是金融巨头的观察名单数据库，该公司将其作为风险和合规工作的一部分。汤森路透(Thomson Reuters)等其他金融公司拥有自己的高风险客户（例如政治风险人士和恐怖分子）数据库。一个 2010 年的小册子指出道琼斯观察名单是为使客户能够对数据库中的任何个人或公司“轻松，准确地识别高风险客户提供详细，最新的配置文件”。这本小册子称，当时数据库有 650,000 个条目，包括现任和前任政治家，受制裁的个人或公司，或被判犯有欺诈等高调金融犯罪的人，或与恐怖主义有联系的任何人。

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：张腾

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158