国家互联网应急中心

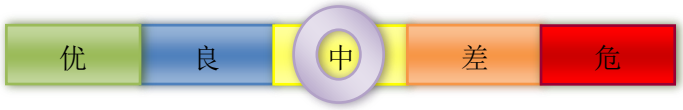
网络安全信息与动态周报

2020 年第 6 期

2 月 3 日-2 月 9 日

CNCERT/CC

本周网络安全基本态势

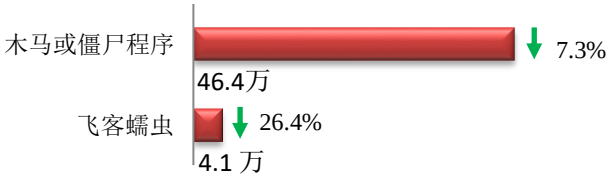


境内感染网络病毒的主机数量	•50.5万	↓ 7.3%
境内被篡改网站总数 其中政府网站数量	•1299 •4	↓ 81.5% ↓ 85.7%
境内被植入后门网站总数 其中政府网站数量	•1395 •4	↓ 17.0% =
针对境内网站的仿冒页面数量	•1205	↑ 1334.5%
新增信息安全漏洞数量 其中高危漏洞数量	•573 •211	↑ 159.3% ↑ 313.7%

= 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 50.5 万个，其中包括境内被木马或被僵尸程序控制的主机约 46.4 万以及境内感染飞客（conficker）蠕虫的主机约 4.1 万。



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。

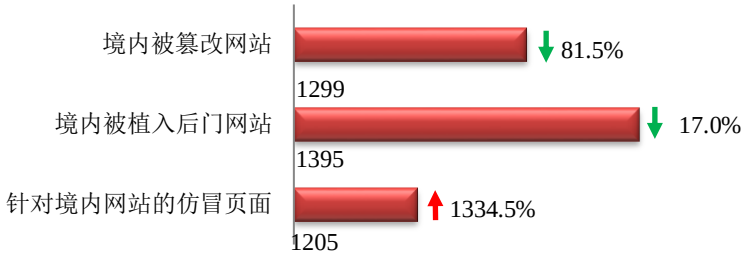
ANVA恶意地址黑名单发布地址

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。

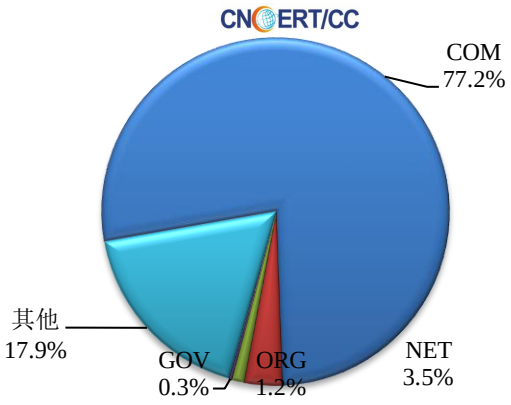
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 1299 个；被植入后门的网站数量为 1395 个；针对境内网站的仿冒页面数量 1205 个。

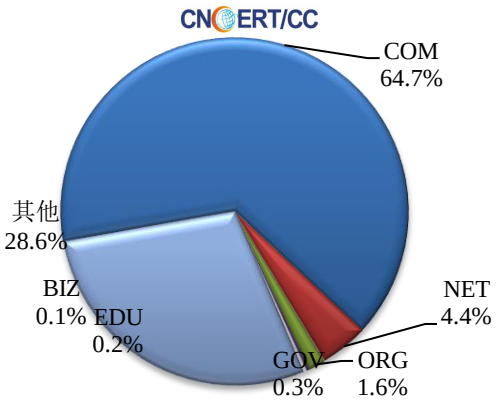


本周境内被篡改政府网站（GOV 类）数量为 4 个（约占境内 0.3%），较上周下降了 85,7%；境内被植入后门的政府网站（GOV 类）数量为 4 个（约占境内 0.3%），与上周持平。

本周我国境内篡改网站按类型分布
(2/3-2/9)

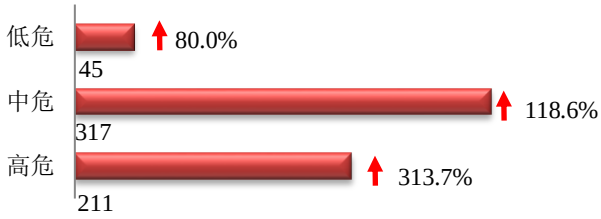


本周我国境内被植入后门网站按类型分布
(2/3-2/9)

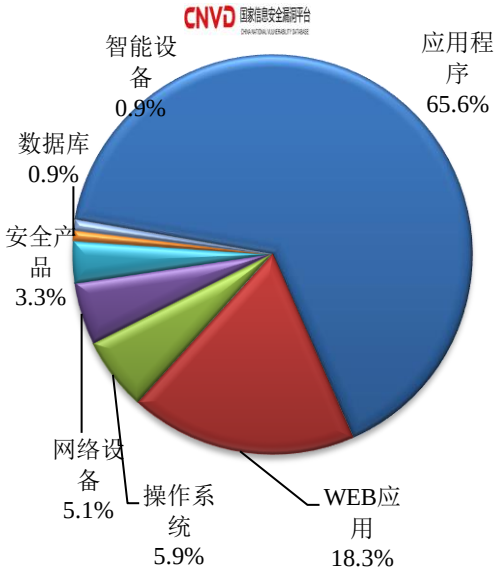


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 573 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
(2/3-2/9)



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 应用和操作系统。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

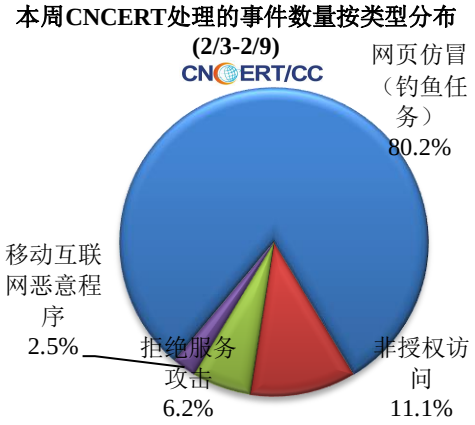
CNVD漏洞周报发布地址

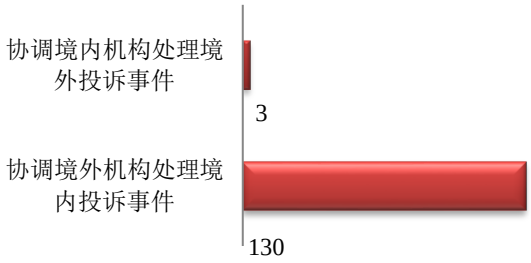
http://www.cnvd.org.cn/webinfo/list?type=4

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。

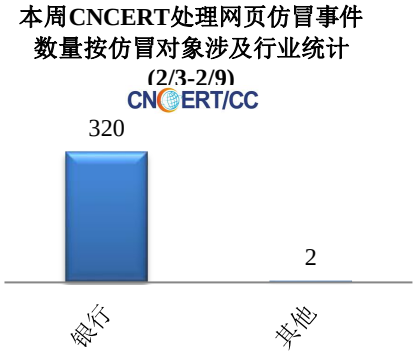
本周事件处理情况

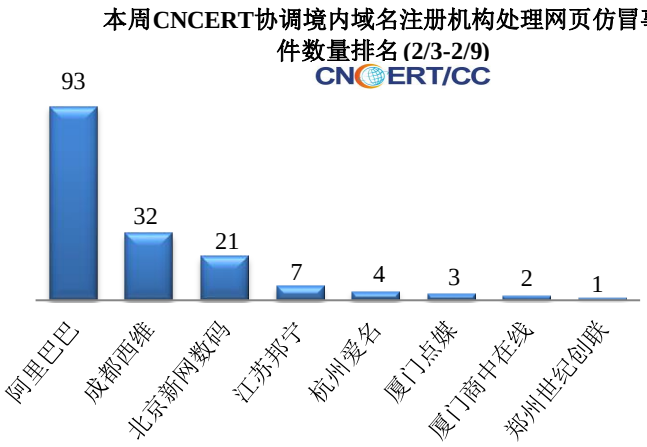
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 353 起，其中跨境网络安全事件 133 起。





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 322 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 320 起和其他事件 2 起。





本周，CNCERT 协调 6 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 7 个。

本周CNCERT协调手机应用商店处理移动互联网恶意代码事件数量排名
(2/3-2/9)

业界新闻速递

1、 网信办：为疫情防控收集的个人信息，不得用于其他用途

2 月 9 日，中央网络安全和信息化委员会办公室发布了《关于做好个人信息保护利用大数据支撑联防联控工作的通知》，针对当下疫情防控工作中所涉及到个人隐私安全问题做了具体要求，除卫生部门依法授权机构外，任何单位、个人都不得借疫情防控为由未经同意收集个人信息。同时收集的个人信息不得用于其他用途，且保障数据安全。

2、 关于近期境外黑客组织拟对我国视频监控系统发起攻击的预警通报

近期，境外黑客组织声称将于 2 月中旬对我国发起网络攻击，以我国多家视频监控系统作为攻击目标，并公布了其掌握的一批相关视频监控系统在用境内 IP 地址。经分析，我国视频监控系统存在一定的漏洞安全隐患和数据泄露风险，可能成为境外黑客发起攻击的薄弱环节。建议各单位和相关用户及早排查风险隐患，提前做好防范应对，具体建议如下：1、清点盘查，做好网络设备资产和数据安全管理，关闭不必要的网络服务和端口，设置强密码，加强登录审计，降低入侵风险；2、查缺补漏，及时跟进在用产品补丁情况，实时检测并修复系统安全漏洞，针对视频监控系统排查弱口令漏洞、后门漏洞、未授权访问漏洞、登录绕过漏洞等风险，并对境外黑客已声称探测的 CVE-2019-0708

（Windows 远程桌面服务远程代码执行漏洞）、CVE-2009-3103（Windows 畸形 SMB 报文远程拒绝服务漏洞）等漏洞进行重点关注，加强边界管理；3、强化预警，建立健全网络安全应急机制，做好数据备份，加大监测力度，发现威胁后，及时进行处置。欢迎向 CNCERT 报送相关情况。

3、 关于防范网络不法分子利用新型肺炎相关主题进行钓鱼邮件入侵的预警通报

近期，网络不法分子利用新型冠状病毒相关题材，冒充国家卫生健康委员会、疫情防疫等相关部门，向我国部分单位和用户投放与新型肺炎疫情相关的钓鱼邮件，钓鱼邮件附带恶意链接与包含恶意代码的 office 文档附件，利用仿冒页面实现对用户信息的收集，诱导用户执行恶意文档中的宏，向受害用户主机上植入木马程序，实现远程控制和信息窃取。请各单位和广大网民强化风险意识，加强安全防范，不给网络不法分子可乘之机，主要安全建议包括：1.不要轻易打开不明来历的电子邮件链接或附件，欢迎向 CNCERT 举报可疑线索；2.已打开钓鱼邮件链接或附件的用户，请及时联系网络安全技术人员，进行风险排查；3.安装杀毒软件，并及时更新病毒库。

4、 50 多万台网络设备的 Telnet 账号密码遭泄露

2 月 6 日，据外媒报道，某黑客论坛里泄露出 51 万互联网服务器、交换机、路由器和物联网等设备的 Telnet 账号密码，经过对这些文件进行核实，一共 16 个 txt 文件，14.5M。据最先发布该消息的网站报道，这份清单是由销售 DDoS 服务的黑产人员在网上发布的。从整体来看，这些数据是使用默认凭证或简单密码对互联网设备进行扫描的结果。这也是网络攻击者构建僵尸网络的常见操作。一旦设备存在弱密码，攻击者就可远程控制住并安装恶意软件（后门或挖矿软件）。

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：徐剑

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315