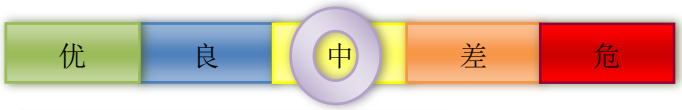
国家互联网应急中心

2019 年第 30 期

7 月 22 日-7 月 28 日

网络安全信息与动态周报

本周网络安全基本态势

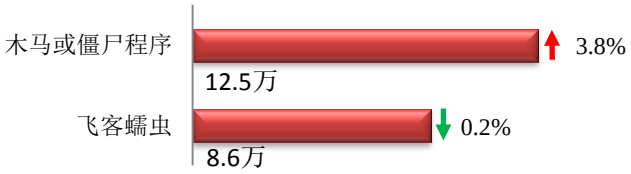


境内感染网络病毒的主机数量	•21.1万	↑2.1%
境内被植入后门网站总数 其中政府网站数量	•4085 •44	↑18.0% ↓4.3%
针对境内网站的仿冒页面数量	•496	↓8.5%
新增信息安全漏洞数量 其中高危漏洞数量	•443 •198	↑6.2% ↑43.5%

=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

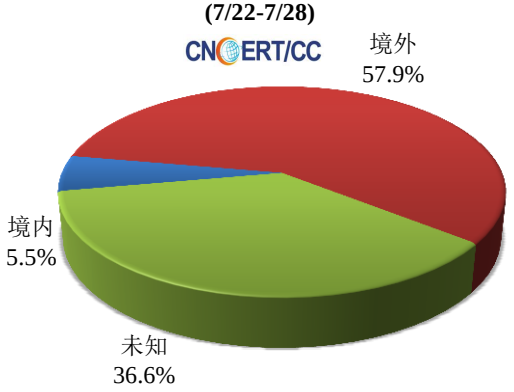
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 21.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 12.5 万以及境内感染飞客（conficker）蠕虫的主机约 8.6 万。

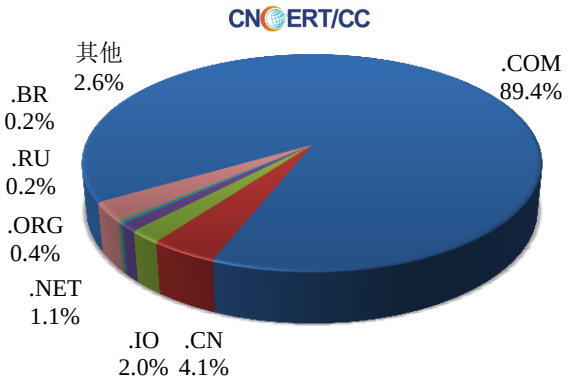


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 14606 个，涉及 IP 地址 4086 个。在 14606 个域名中，有 57.9%为境外注册，且顶级域为.com 的约占 89.4%；在 4086 个 IP 中，有约 49.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 730 个 IP。

本周放马站点域名注册所属境内外分布
(7/22-7/28)



本周放马站点域名所属顶级域的分布
(7/22-7/28)



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。

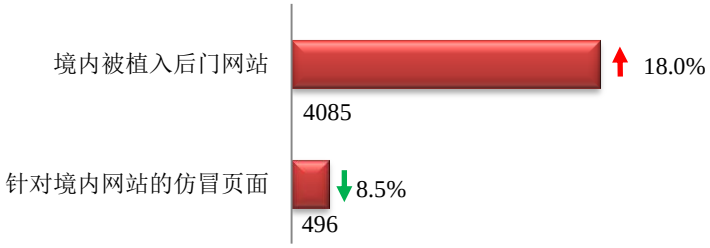
ANVA恶意地址黑名单发布地址

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。

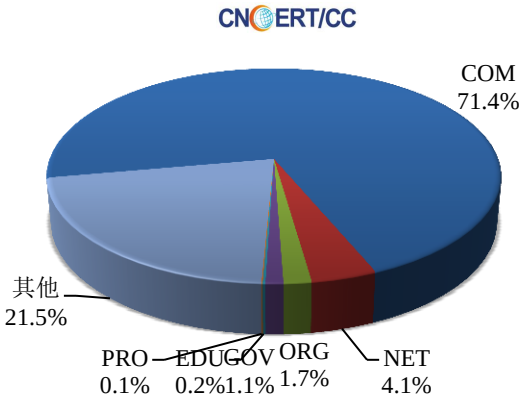
本周网站安全情况

本周 CNCERT 监测发现境内被植入后门的网站数量为 4085 个；针对境内网站的仿冒页面数量 496 个。



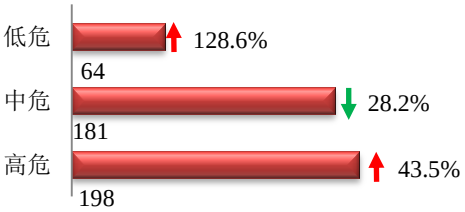
境内被植入后门的政府网站（GOV 类）数量为 44 个（约占境内 1.1%），较上周环比下降 4.3%；针对境内网站的仿冒页面涉及域名 361 个，IP 地址 187 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被植入后门网站按类型分布
(7/22-7/28)

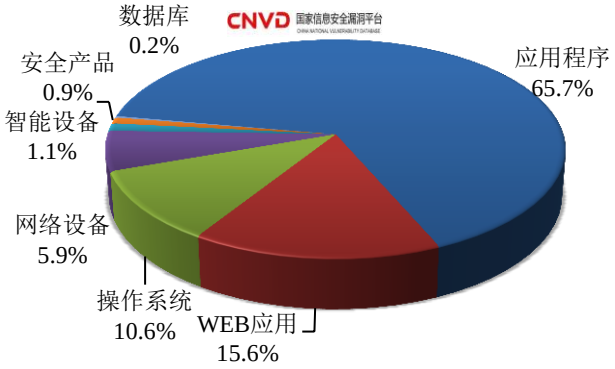


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 443 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
(7/22-7/28)



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 应用漏洞和操作系统漏洞。

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

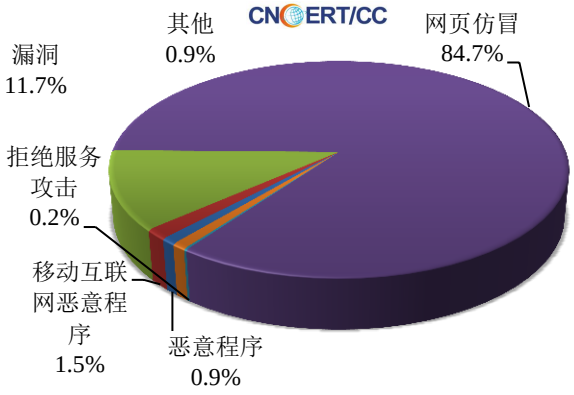
http://www.cnvd.org.cn/webinfo/list?type=4

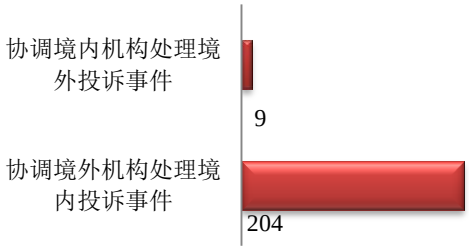
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 537 起，其中跨境网络安全事件 213 起。

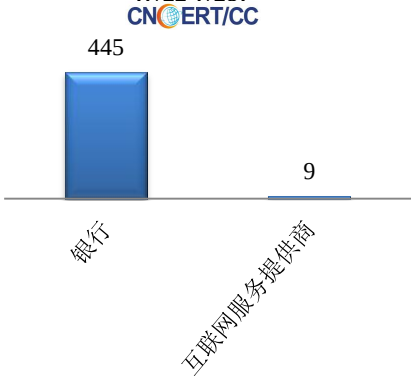
本周CNCERT处理的事件数量按类型分布 (7/22-7/28)



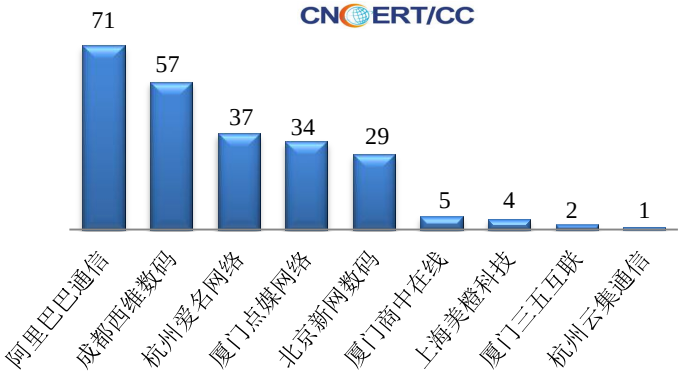


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 454 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 445 起和互联网服务提供商仿冒事件 9 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (7/22-7/28)

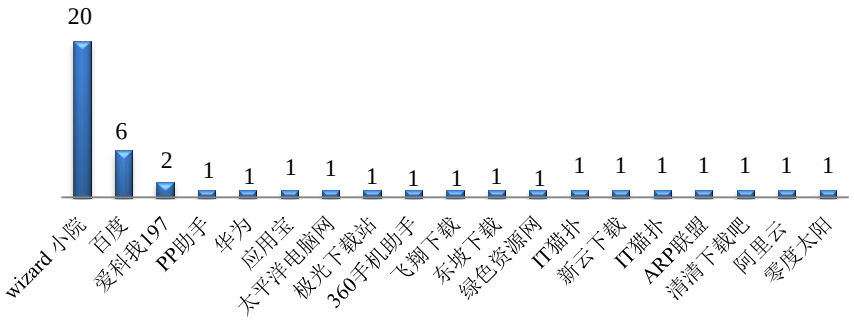


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (7/22-7/28)



本周，CNCERT 协调 19 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 44 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
(7/22-7/28)



业界新闻速递

1、美国国安局将设立网络安全理事会

新华社华盛顿 7 月 23 日消息 美国国家安全局 23 日宣布，将于 10 月成立一个名为“网络安全理事会”的下设分支机构，旨在整合情报收集、网络防御等任务。网络安全理事会将是一个重要分支机构，负责整合国安局在情报收集和网络防御方面的任务，并负责“预防和消除针对美国国家安全系统和国防工业基地的威胁”。网络安全理事会将使国安局能够“重新定义”其在网络安全方面的使命。这一网络安全理事会将由安妮·纽伯格领导，她曾担任美国国安局的首位首席风险官。

2、巴西总统社交媒体账号被盗

E 安全 7 月 28 日消息 巴西四名黑客因涉嫌入侵 1000 多个 Telegram 账户被捕。受到入侵的包括巴西总统雅伊尔·博索纳罗(Jair Bolsonaro)、司法部长塞尔吉奥·莫罗(Sergio Moro)和经济部长保罗·格德斯(Paulo Guedes)所使用的账户。黑客们在登陆目标账户时会要求使用语音验证码进行验证。如果账号所绑定手机号正在通话中或连续三次未被接听，那么该验证码将会以留言的方式发送到该手机号的语音信箱中。接下来，黑客们利用了 voip provider 来假冒该手机号，然后用此号码拨打电信公司的语音信箱服务，并尝试输入语音信箱的默认密码（多为 0000 或 1234）来进入此语音邮箱。在成功听到含有 telegram 账户语音验证码的留言后，黑客们会使用这条验证码登录受害者的账户，并将帐户绑定到他们的设备上。

3、美国著名征信公司 Equifax 就数据泄漏与当局达成 5.25 亿美金和解协议

美国著名征信公司 Equifax 同美国消费者金融保护局（Consumer Financial Protection Bureau, CFPB）、联邦贸易委员会（Federal Trade Committee）、四十八个州、哥伦比亚特区以及波多黎各自由邦，就 Equifax 于 2017 年发生的数据泄露事件而引发的调查与诉讼达成和解协议。

4、韩国门户 Naver 因未实行内外网分离被罚 3000 万韩元

cbBeta.COM7 月 23 日消息 Naver 因未履行维护电子金融交易安全的义务，被韩国金融监督局处以 3000 万韩元的罚款 。根据现行《电子金融交易法》和《电子金融监督规定》，为防止金融机构的信息处理系统和信息通信网络遭受黑客入侵等威胁行为，应当将连接内网的业务用系统与外网进行分离操作。但是 Naver 在总部员工终端设备等内部系统没有完成内外网分离的情况下，进行了联网操作。

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：贾世琳

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315