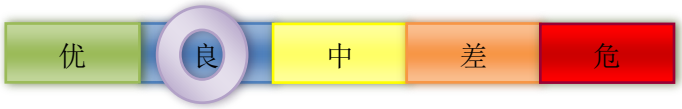
国家互联网应急中心

2019 年第 8 期
2 月 18 日-2 月 24 日

网络安全信息与动态周报

本周网络安全基本态势

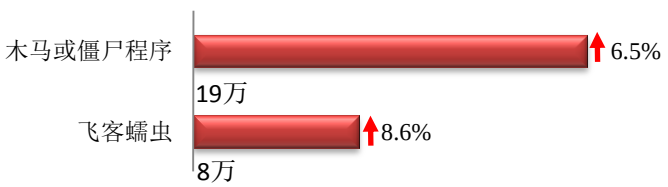


境内感染网络病毒的主机数量	•27.0万	↑6.5%
境内被篡改网站总数 其中政府网站数量	•580 •44	↑18.4% ↑22.2%
境内被植入后门网站总数 其中政府网站数量	•445 •11	↑12.4% ↑175.0%
针对境内网站的仿冒页面数量	•1416	↑78.1%
新增信息安全漏洞数量 其中高危漏洞数量	•194 •48	↓11.0% ↓22.6%

=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

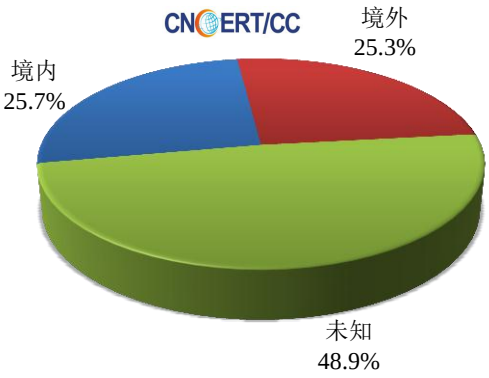
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 27.0 万个，其中包括境内被木马或被僵尸程序控制的主机约 19.0 万以及境内感染飞客（conficker）蠕虫的主机约 8.0 万。

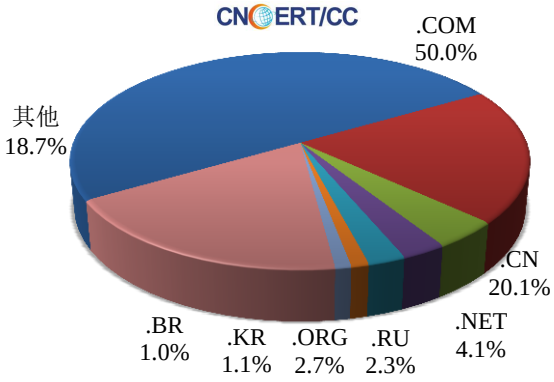


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 2882 个，涉及 IP 地址 6220 个。在 2882 个域名中，有 25.3%为境外注册，且顶级域为.com 的约占 50.0%；在 6220 个 IP 中，有约 62.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 803 个 IP。

本周放马站点域名注册所属境内外分布
(2/18-2/24)



本周放马站点域名所属顶级域的分布
(2/18-2/24)



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。

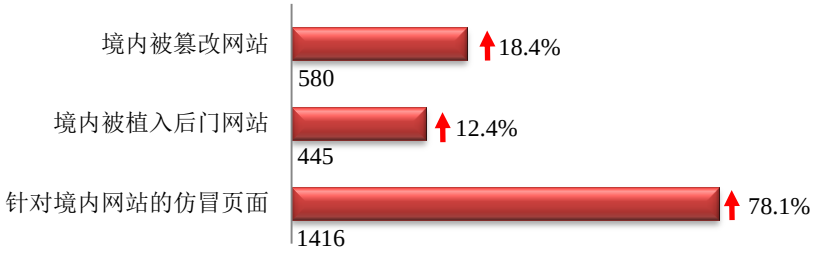
ANVA恶意地址黑名单发布地址

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。

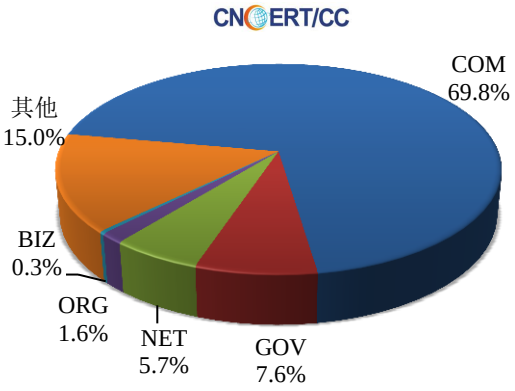
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 580 个；境内被植入后门的网站数量为 445 个；针对境内网站的仿冒页面数量 1416 个。

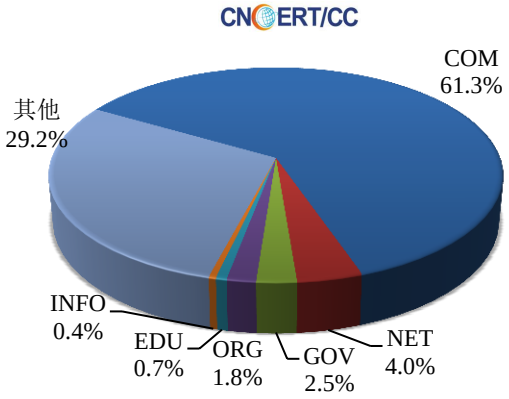


本周境内被篡改政府网站（GOV 类）数量为 44 个（约占境内 7.6%），较上周环比上升了 22.2%；境内被植入后门的政府网站（GOV 类）数量为 11 个（约占境内 2.5%），较上周环比上升了 175.0%；针对境内网站的仿冒页面涉及域名 401 个，IP 地址 244 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(2/18-2/24)

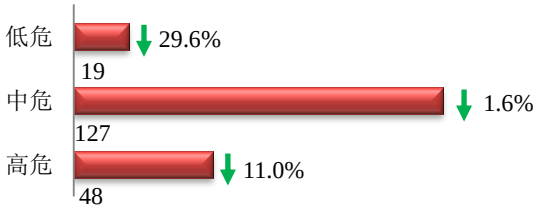


本周我国境内被植入后门网站按类型分布
(2/18-2/24)

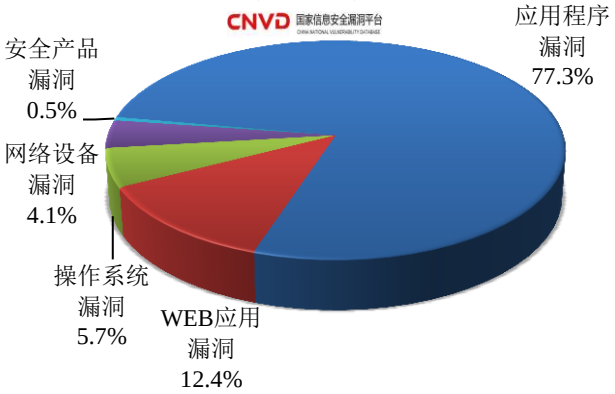


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 194 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
(2/18-2/24)



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

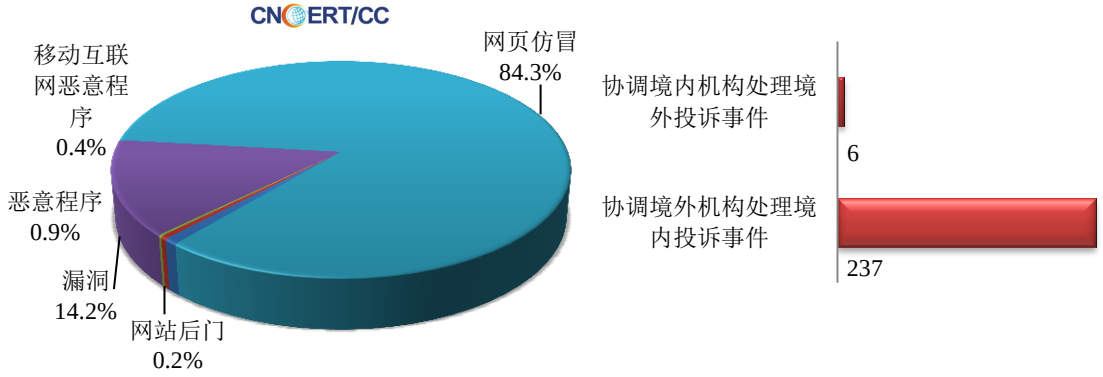
http://www.cnvd.org.cn/webinfo/list?type=4

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 452 起，其中跨境网络安全事件 243 起。

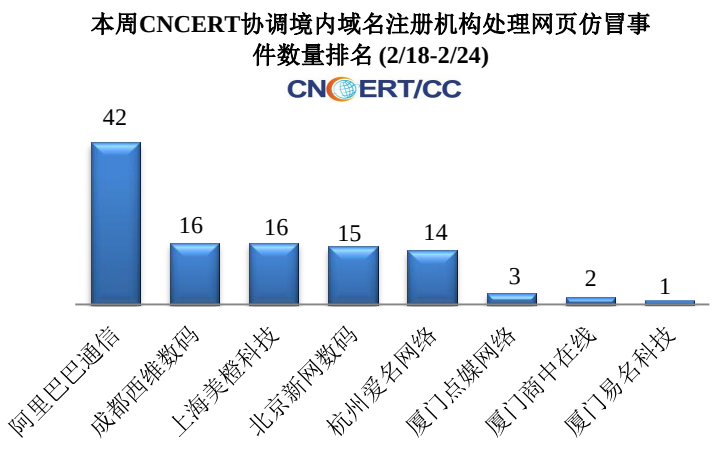
本周CNCERT处理的事件数量按类型分布 (2/18-2/24)



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 381 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 374 起和政府公益仿冒事件 4 起。

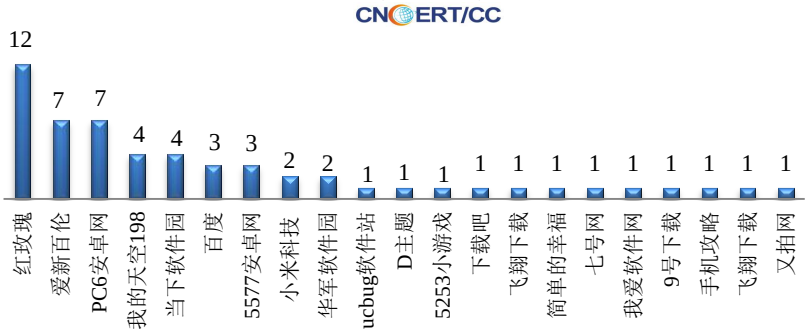
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (2/18-2/24)

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 (2/18-2/24)



本周，CNCERT 协调 21 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 56 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
(2/18-2/24)



业界新闻速递

1、白宫出台针对恐怖分子流动的战略，生物识别技术是关键

E 安全 2 月 24 日消息 美国白宫于 2 月 20 日发布了《打击恐怖分子流动的国家战略》（National Strategy to Combat Terrorist Travel），该战略计划靠身份验证和生物识别身份系统来探测和阻止恐怖分子的流动。政府将为州、地方和部落提供恐怖主义人员的身份和流动数据，以及识别恐怖分子的工具和技术。相关信息来自最新的身份管理系统、可疑人员流动数据以及人员的生物特征和案底数据。 根据这份文件，对人员的审查包括对监视名单和威胁信息的记录或生物特征进行匹配，以及用于解决潜在匹配和误报的手动和自动过程。 美国将大范围使用该技术。乘坐国际航班的乘客的照片会与一个临时的云数据库进行对比，美国境内每位行人在十字路口的照片，也会与他们的证件照片（如护照）作比较。

2、瑞典医疗热线泄露 270 万条通话记录：涉及诸多敏感信息

黑客视界 2 月 19 日消息 拨打给瑞典医疗保健热线 1177 Vårdguiden 的 270 万条通话录音信息在网络上曝光。长达 17 万小时、包含极其敏感信息的呼叫音频存储在开放的 Web 服务器上，并且没有经过任何的加密和身份认证，意味着互联网上的任意用户都可以通过 Web 浏览器完全访问这些个人信息，其中包括患者的疾病、目前服用的药物以及相关病史等敏感信息。甚至在部分通话中要求描述孩子的症状并要求提供他们的社会安全号码。部分文件中还包括这些通话的个人电话号码。中出现了大约 57,000 个号码，其中许多是呼叫者的个人号码，因此可以轻松地将信息与特定人员匹配。目前还不清楚这些电话可用多长时间，谁应该为违规行为负责，以及是否有任何不良恶意成员已经访问过这些信息。

3、印度国有液化石油气公司 670 万用户信息遭泄露，包括 Aadhaar 号码

Hackeye.NET2 月 21 日消息 近日，法国安全研究员在一名不愿透露姓名的印度安全研究员的帮助下发现了印度国有液化石油气公司 Indane 官方网站的一个安全漏洞。该漏洞被证实会导致数百万用户的个人信息泄露，包括他们的 Aadhaar 号码。Aadhaar 号码是印度身份证管理局（UIDAI）向每一位印度公民发行的一个唯一的 12 位身份证明编号，并与姓名、出生日期和生物特征信息（如指纹、虹膜）等基本人口信息相关联，而这些数据被集中存储在印度国家生物身份识别系统（UID，又称 Aadhar）中。每一位印度公民都可以通过在线登录该系统来进行身份识别，同时还能通过该系统来进行与医疗、社保、培训、驾照、就业等相关服务的申请。另一方面，印度政府各部门也可以通过该系统来进行有针对性的补贴和福利发放，对公民健康状况等进行监测，进而有效提供医疗和防疫等公共服务。数据泄露源于 Indane 官网的一个漏洞。该漏洞的存在使得任何人都能够访问与 Indane 旗下经销商相关的数十万用户的个人信息，且不需要任何身份验证。

4、黑客在暗网上出售 7 万张巴基斯坦银行信用卡 PIN 码

E 安全 2 月 24 日消息 研究人员在网上发现了两个新的数据库，其中包含了 7 万个巴基斯坦银行的信用卡/借记卡数据，这些数据在地下市场上出售。根据发现该数据库的 Group-IB 估计，这些数据价值近 350 万美元，是过去 6 个月巴基斯坦银行在暗网上大卖的数据之一。目前这些数据仍在暗网中出售，所有数据均为巴基斯坦 Meezan 银行磁条所载信息的未经授权的数字副本。第一个被发现的数据库包含 1535 张标题为«PAKISTAN-D+P-01»的信用卡数据，其中 1457 张由 Meezan 银行发行，这些信用卡数据于 2019 年 1 月 24 日开始出售。第二个数据库比第一个数据库大，包含巴基斯坦银行 67654 张银行卡的详细信息。

5、WinRAR 被曝严重安全漏洞 5 亿用户受影响

cnBeta.COM2 月 21 日消息 在享誉全球成为必备装机软件的同时，过去 19 年以来 WinRAR 也深受各种严重安全漏洞的负面影响。根据安全公司 Check Point 研究人员披露的细节，在 WinRAR 的 UNACEV2.dll 代码库中发现严重安全漏洞，而该库自 2005 年以来就一直没有被主动使用过。WinRAR 在打开“booby-trapped”（诡雷代码）文件之后允许技术娴熟的攻击者执行“任意恶意代码”。 简单来说，该漏洞允许安全专家绕过权限提升就能运行 WinRAR，而且可以直接将恶意文件放进 Windows 系统的启动文件夹中。这就意味着当用户下次重新开机的时候，这些恶意文件就能自动运行，让安全专家“完全控制”受害者的计算机。安全专家表示，全球有超过 5 亿用户受到 WinRAR 漏洞影响。

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：吕利锋

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158