

网络安全信息与动态周报

本周网络安全基本态势



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 57.3 万个，其中包括境内被木马或被僵尸程序控制的主机约 42.0 万以及境内感染飞客（conficker）蠕虫的主机约 15.3 万。

木马或僵尸程序

42.0万 ↑ 5.0%

飞客蠕虫

15.3万 ↓ 8.7%

本周 CNCERT 捕获的新增网络病毒文件，按网络病毒名称统计新增 1 个，按网络病毒家族统计无新增。

新增网络病毒名称

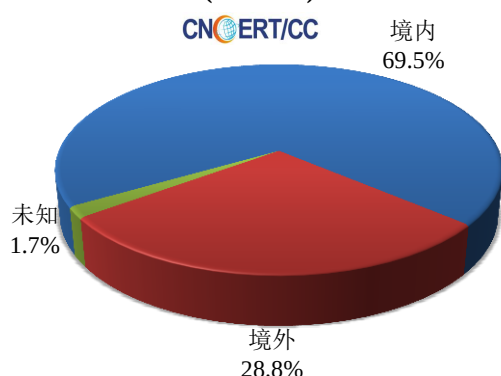
1 ↑

新增网络病毒家族

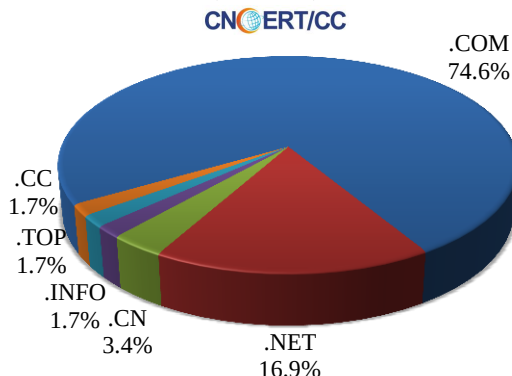
0 =

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 59 个，涉及 IP 地址 329 个。在 59 个域名中，有 28.8% 为境外注册，且顶级域为 .com 的约占 74.6%；在 329 个 IP 中，有约 4.9% 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 2 个 IP。

本周放马站点域名注册所属境内外分布
(8/21-8/27)



本周放马站点域名所属顶级域的分布
(8/21-8/27)



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

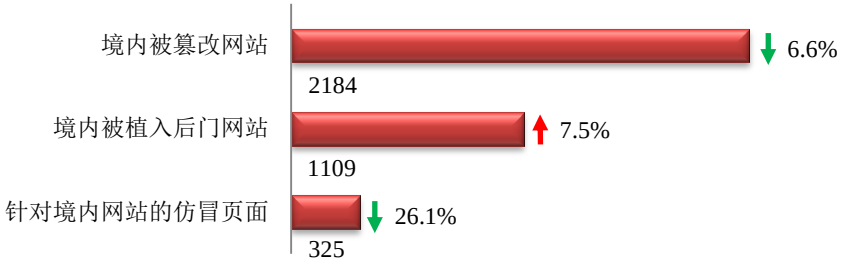
<http://www.anva.org.cn/virusAddress/listBlack>

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。

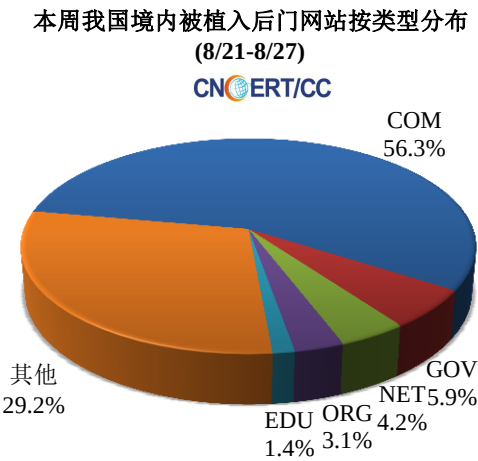
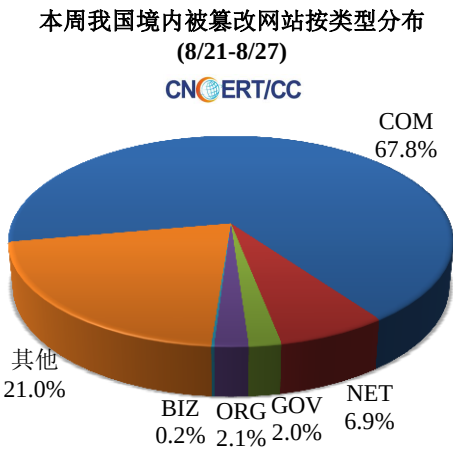


本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2184 个；境内被植入后门的网站数量为 1109 个；针对境内网站的仿冒页面数量为 325。

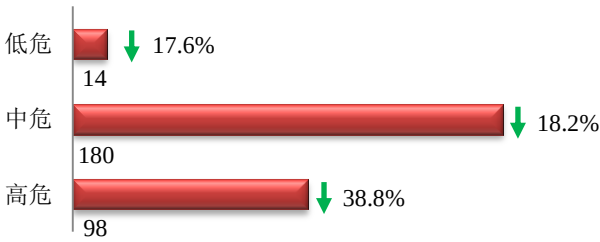


本周境内被篡改政府网站（GOV 类）数量为 44 个（约占境内 2.0%），较上周环比下降了 20.0%；境内被植入后门的政府网站（GOV 类）数量为 65 个（约占境内 5.9%），较上周环比下降了 9.7%；针对境内网站的仿冒页面涉及域名 272 个，IP 地址 116 个，平均每个 IP 地址承载了约 3 个仿冒页面。

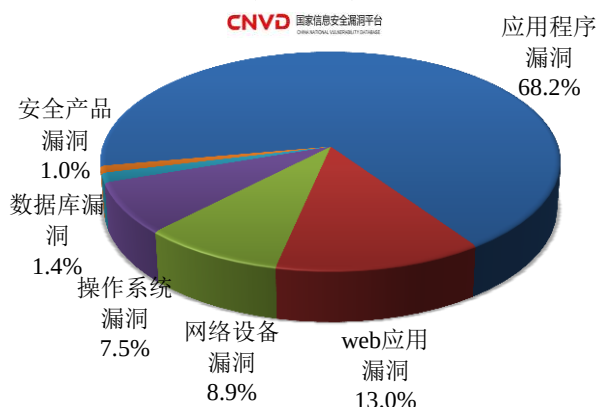


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 292 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
(8/21-8/27)



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

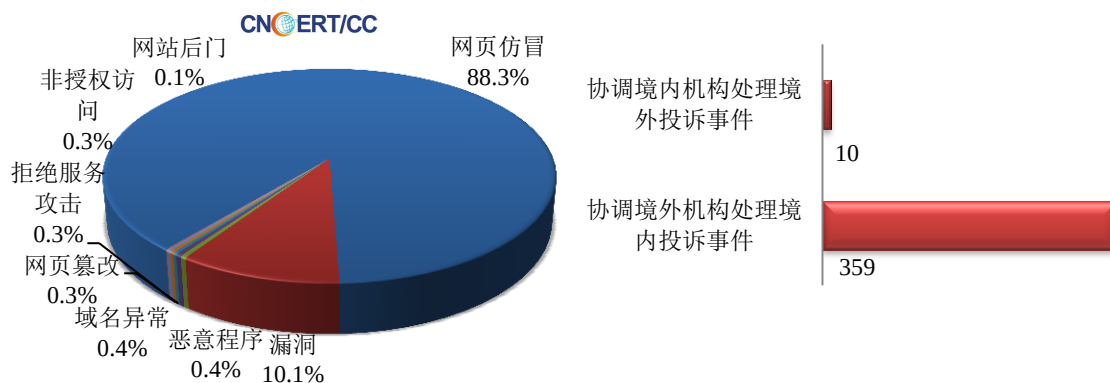
<http://www.cnvd.org.cn/webinfo/list?type=4>

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 794 起，其中跨境网络安全事件 369 起。

本周CNCERT处理的事件数量按类型分布
(8/21-8/27)



协调境内机构处理境外投诉事件

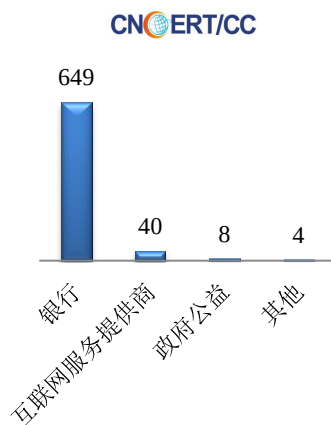
10

协调境外机构处理境内投诉事件

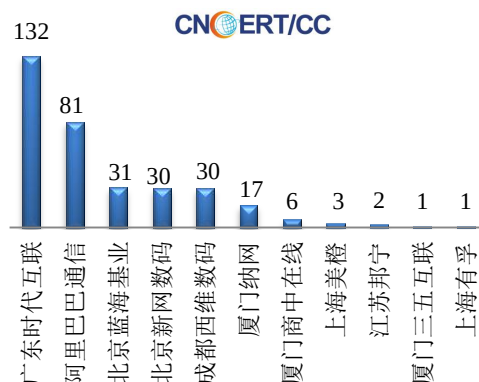
359

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 701 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 649 起和互联网服务提供商仿冒事件 40 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(8/21-8/27)

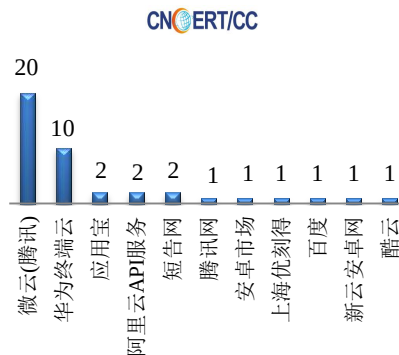


本周CNCERT协调境内域名注册机构处理网页
仿冒事件数量排名 (8/21-8/27)



本周，CNCERT 协调 11 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 42 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
(8/21-8/27)



业界新闻速递

1、国家网络安全学院项目武汉开建

中国日报网 8 月 24 日消息 国家网络安全学院及配套的超算数据中心、科技孵化园等一批项目 8 月 23 日在武汉市临空港经济技术开发区集中开工建设。项目总投资达到 216 亿元。这标志着由中央网信办扶持的首个“国家网络安全人才与创新基地”整体进入实质性建设阶段。国家网络安全学院项目总用地面积 1500 亩，总投资 50 亿元，规划建设网络安全学院、培训学院和研究院。项目计划 2018 年 11 月完成结构封顶，2019 年 6 月建成

投入运营,将为 1 万人提供教育培养和专业培训的学习研究及生活的场所,为打造网络安全人才提供重要载体。与国家网络安全学院项目配套的展示中心、国际人才社区、超算数据中心等一批项目当日也同步开工建设。

2、美国国家基础设施顾问委员会警告防范“911”网络攻击

E 安全 8 月 24 日消息 美国国家基础设施顾问委员会（简称 NIAC）周二通过的一份报告，指出美国处于 911 前的紧迫时刻，在大型攻击到来之前，美国必须抓住稍纵即逝的微小机会有效协调资源。报告警告称，美国未做好准备应对针对电网、通信系统等关键基础设施的灾难性网络攻击。顾问委员会成员包括公司高管和前政府高级官员投票通过这份报告，建议美国建立独立的通信网络以支持关键系统，并采取措施解密网络安全威胁信息，以便前线基础设施运营商可利用这些信息防御攻击。报告提到的建议措施包括，强化劳动力、改进机器对机器信息共享并简化安全调查程序，从而消除私有部门和承包商担负的不对称工作积压。NIAC 建议由白宫国家安全顾问监督关键基础设施网络安全，此外还提到能源部的公共/私有网络安全风险信息共享计划和国土安全部网络信息共享与合作计划。报告指出，当美国基础设施遭遇国家攻击时，私营企业在网络中处于防御第一线。

3、亚马逊 AWS 服务器信息泄露 180 万选民信息曝光

新浪网 8 月 21 日消息 北京时间 8 月 21 日早间消息，美国一家选票计算机公司上周四证实，他们泄露了 180 多万伊利诺伊州居民的个人信息。该公司已经上报伊利诺伊州政府和美国联邦调查局（FBI），而泄露的信息中包含选民姓名、地址、出生日期、部分社会安全号和部分党派关系，此外还包含一些驾驶执照和州身份证信息。网络安全公司 UpGuard 的乔·亨得利（Jon Hendren）在一台未受密码保护的亚马逊网络服务（AWS）设备上发现了此项漏洞。磁盘分析师克里斯·维客利（Chris Vickery）随后下载了这些选票数据，并判断这些数据来自 Election Systems & Software（以下简称“ES&S”）——这家公司为至少 42 个州提供选票计算机和服务。ES&S 在声明中表示，该公司也已经在 UpGuard 的协助下自行展开“彻底调查”。该公司称，AWS 服务器并未包含任何投票信息，也不会对任何选举结果产生影响。

4、黑客使用.fish 域名网站来骗取法国银行客户

cnBeta.COM 8 月 22 日消息 网络安全公司 Netcraft 发现黑客使用.fish 域名网站来骗取法国银行客户，他们发现一个采用.fish 域名的网站伪装成法国银行网站来对客户进行钓鱼攻击。当有人访问 parser.fish 时，他们将被重定向到一个越南网站，伪装成法国银行 BRED，同时试图盗取用户的银行证书。经过查他们发现，Parser.fish 域名在多云托管服务 Tucows 上匿名注册，这并非不平常，但这就几乎不可能找出谁拥有该网站，以及它是如何被黑掉的，最有可能的解释是该网站遭到黑客入侵。幸运的是，目前该网站已经被清除了恶意代码。.fish 成为顶级域名已经有一段时间了。它是几个新顶级域名之一，如.sexy、.tech 和.xyz，它们和地理位置没有关系，.fish 顶级域名主要针对那些对水生生物感兴趣的用户。

5、维基解密：CIA 利用虚假软件升级系统来监控合作伙伴

凤凰网 8 月 25 日消息 据科技博客 The Verge 北京时间 8 月 25 日报道，维基解密今天公布的一份文件显示，美国中央情报局（CIA）曾秘密创建了一个虚假的软件更新系统，用以暗中监视情报合作伙伴，而这一秘密项

目最早可以追溯到 2009 年。这一秘密项目名为“ExpressLane”，该项目与 CIA 的生物识别系统一道被 CIA 部署给合作机构。理论上讲，只有经这些合作伙伴同意，CIA 才能够访问特定的生物识别数据，但在秘密部署“ExpressLane”项目后，CIA 能够在合作伙伴不知情的情况下暗中获取相关信息。据悉，“ExpressLane”被伪装成一款软件升级，由 CIA 技术人员亲自送给合作伙伴。但文件清晰地表明，这个项目本身实质上并未改变系统。相反，该项目能够将系统的数据传输到一个 U 盘上，供 CIA 查询使用，从而查看合作伙伴的系统是否设置了障碍。如果合作伙伴拒绝了虚假的更新软件，那么就会有一个隐藏的 kill 开关启动，让 CIA 有权在一段时间后关闭整个系统，并需要 CIA 技术人员亲自访问帮助恢复系统。

6、加密货币勒索软件 Miner 可利用 WMI 与“永恒之蓝”肆意传播

HackerNews.cc 8 月 23 日消息 据外媒 8 月 21 日报道，趋势科技（Trend Micro）研究人员近期发现加密货币勒索软件 Miner，允许黑客利用 Windows 管理工具 WMI 与安全漏洞“永恒之蓝（EternalBlue）”进行肆意传播。据悉，该勒索软件首次于今年 7 月发现，受其影响最严重的国家包括日本（43.05%）、印度尼西亚（21.36%）、台湾（13.67%）、泰国（10.07%）等。研究人员表示，该勒索软件使用 WMI 作为无文件持久性机制，即由 WMI Standard Event Consumer 脚本应用程序（scrcons.exe）执行。此外，Miner 还使用 EternalBlue 漏洞感染系统网络。研究显示，无文件 WMI 脚本与 EternalBlue 的结合可以使 Miner 隐蔽持久的感染目标设备。Miner 的感染流程分为多个阶段。首先，Miner 感染目标系统后会通过 EternalBlue 漏洞删除并运行系统后门（BKDR_FORSHARE.A）；其次，系统在安装各种 WMI 脚本后，会将其连接到 C&C 服务器并获取指令；最终，目标系统将下载运行该恶意软件与其相关组件进行肆意传播。

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。截止 2016 年，CNCERT 与 69 个国家和地区的 185 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：张帅



网址: www.cert.org.cn

email: cncert_report@cert.org.cn

电话: 010-82990158