国家互联网应急中心

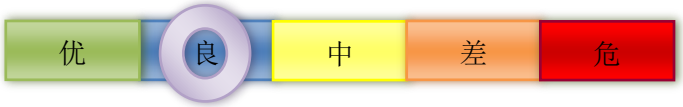
2018 年第 34 期

8 月 20 日-8 月 26 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

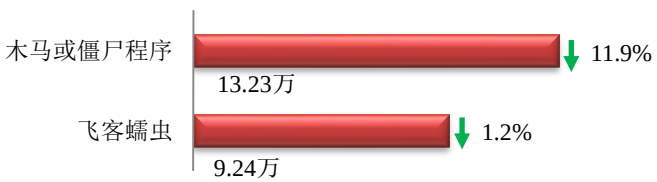


境内感染网络病毒的主机数量	•22.47万	↓ 7.8%
境内被篡改网站总数 其中政府网站数量	•932 •34	↑ 3.6% ↓ 8.1%
境内被植入后门网站总数 其中政府网站数量	•806 •19	↑ 12.1% ↑ 18.8%
针对境内网站的仿冒页面数量	•1582	↑ 55.4%
新增信息安全漏洞数量 其中高危漏洞数量	•230 •75	↓ 16.1% ↓ 29.9%

═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

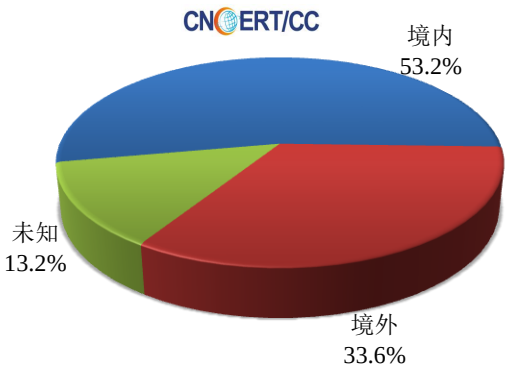
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 22.47 万个，其中包括境内被木马或被僵尸程序控制的主机约 13.23 万以及境内感染飞客（conficker）蠕虫的主机约 9.24 万。

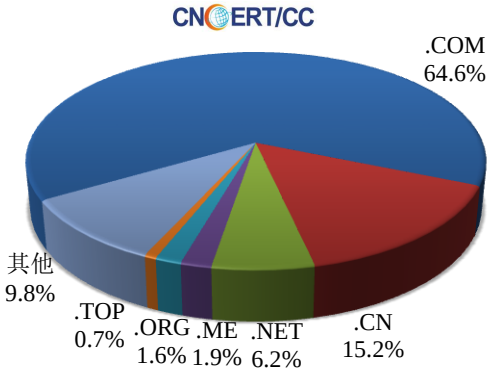


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1490 个，涉及 IP 地址 94495 个。在 1490 个域名中，有 33.6%为境外注册，且顶级域为.com 的约占 64.6%；在 94495 个 IP 中，有约 35.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 360 个 IP。

本周放马站点域名注册所属境内外分布
(8/20-8/26)



本周放马站点域名所属顶级域的分布
(8/20-8/26)



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。

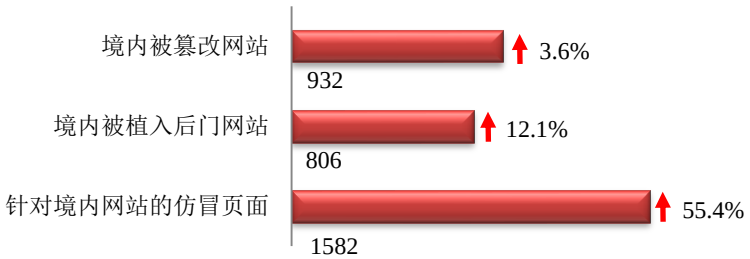
ANVA恶意地址黑名单发布地址

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。

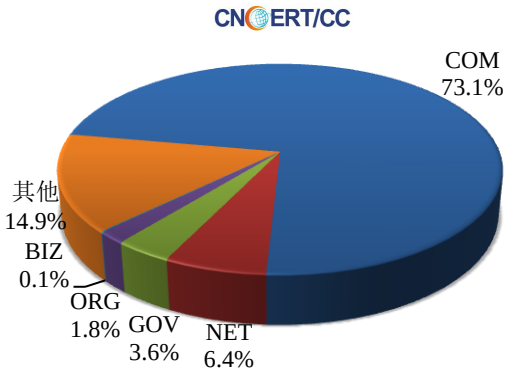
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 932 个；境内被植入后门的网站数量为 806 个；针对境内网站的仿冒页面数量为 1582。

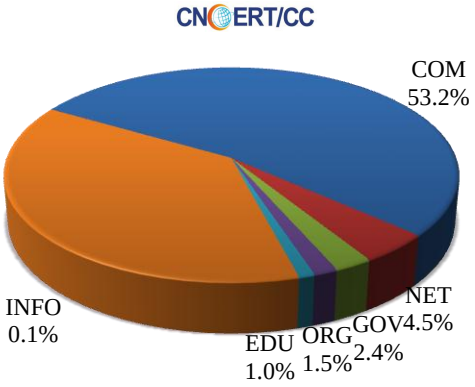


本周境内被篡改政府网站（GOV 类）数量为 34 个（约占境内 3.6%），较上周环比下降了 8.1%；境内被植入后门的政府网站（GOV 类）数量为 19 个（约占境内 2.4%），较上周环比上升了 18.8%；针对境内网站的仿冒页面涉及域名 582 个，IP 地址 265 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(8/20-8/26)

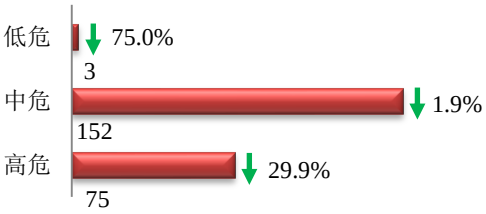


本周我国境内被植入后门网站按类型分布
(8/20-8/26)

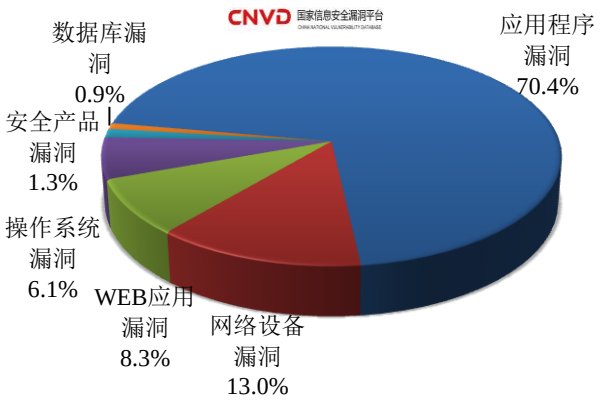


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 230 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
(8/20-8/26)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是网络设备漏洞和 WEB 应用漏洞。

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

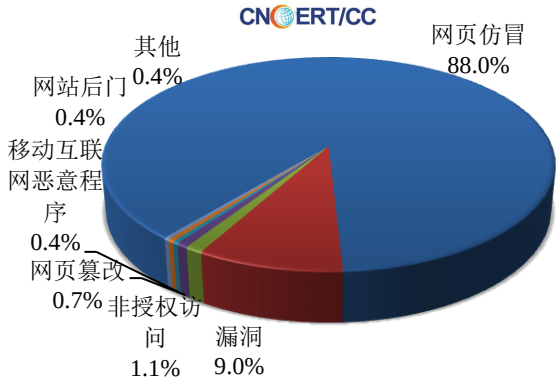
http://www.cnvd.org.cn/webinfo/list?type=4

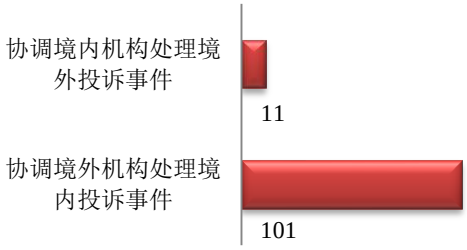
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 543 起，其中跨境网络安全事件 112 起。

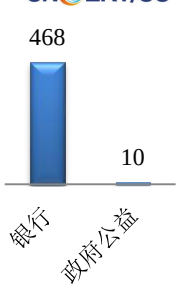
本周CNCERT处理的事件数量按类型分布 (8/20-8/26)



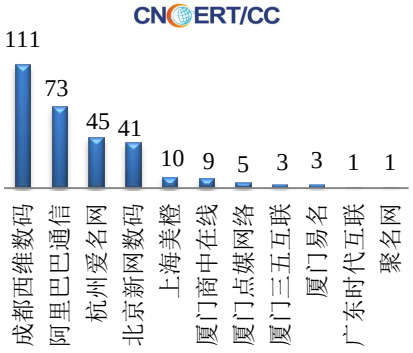


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 478 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 468 起和政府公益仿冒事件 10 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(8/20-8/26)

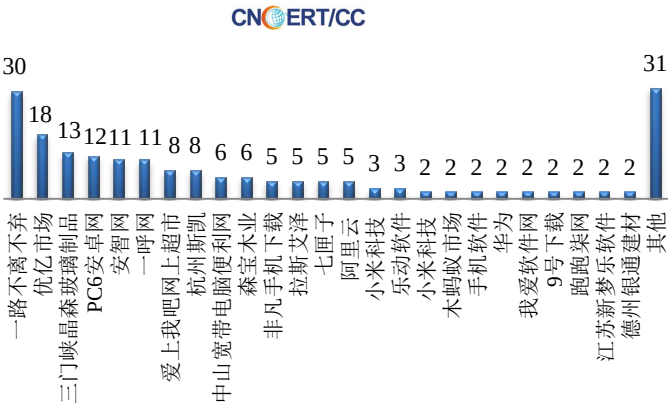


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (8/20-8/26)



本周，CNCERT 协调 26 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 198 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
(8/20-8/26)



业界新闻速递

1、金融业网络安全攻防比赛成功举办

中国金融新闻网 8 月 24 日消息 中国人民银行以及公安部、银保监会、证监会有关部门联合主办的金融业网络安全攻防比赛 8 月 23 日在北京圆满落幕。中国人民银行党委委员、副行长范一飞莅临比赛现场并为获奖队伍颁奖。范一飞表示，当前金融行业网络安全形势复杂严峻，在国家有关部门的指导下，各金融机构不断加强关键信息基础设施保护，成功抵御了各类外部网络攻击。新时期金融行业要进一步提高认识，认真贯彻落实习近平总书记网络强国战略思想，培养更多优秀网络安全人才，切实筑牢行业网络安全屏障，有效保障金融安全。据了解，本次比赛覆盖范围广泛，特别是一些地方中小金融机构也积极参与，较好地达到了“以赛代训，以赛促学”的目的，为培养金融行业网络安全人才、提升行业信息技术风险防控能力、促进行业网络安全技术发展起到了积极推动作用。银行、证券、保险等行业 2000 余名技术骨干组成的 510 支代表队参加了初赛，其中 20 支代表队脱颖而出进入决赛。经过激烈角逐，来自蚂蚁金服、建设银行、中国银行的代表队获得本次比赛一等奖。中央网信办、公安部、银保监会、证监会及各参赛金融机构有关负责同志赴现场观摩比赛并出席颁奖仪式。

2、美国 22 个州联名诉 FCC 要求恢复“网络中立”规则

网易 8 月 21 日消息 据国外媒体报道，当地时间周一晚些时候，一个由 22 名州检察长和哥伦比亚特区组成的小组，要求美国一家上诉法院恢复奥巴马政府 2015 年出台的具有里程碑意义的网络中立规则（Net neutrality）。美国联邦通信委员会（FCC）去年 12 月投票表决，废除了关于禁止互联网服务提供商阻塞、限制流量或提供付费快车道（也称付费优先次序）的规定。FCC 表决通过的新规定于 6 月初生效，新规定授予互联网服务提供商广泛的新权力，改变了美国人使用互联网的方式。各州认为，FCC 的新规定会伤害消费者。这些州还表示，FCC 没有任何“有效权威”来越过州及其保护网络中立性的地方法律。截止目前为止，有六个州的州长签署了关于

网络中立的行政命令，三个州颁布了网络中立法律。

3、美国陆军正在考虑建立人工智能任务组

网易 8 月 24 日消息 美国陆军首席信息官（CIO）布鲁斯·克劳福德（Bruce Crawford）表示，美国陆军可能在未来 90 天内建立一支人工智能任务组，以帮助开发必要的专业知识，并为未来的战争做好准备。此项目还将创建一个云计算顾问委员会。克劳福德在佐治亚州奥古斯塔举行的 AFCEA TechNet Augusta 会议期间提到了潜在的任务组，他将特别任务组与国防部建立的联合人工智能中心（JAIC）联系在一起，该部门的首席信息官 Dana Deasy 领导了这项工作。他强调，该项目并不是在寻找一种“一刀切”的云计算解决方案。FFRDC 将“确保我们在未来 6 到 12 个月内开发的混合云解决方案是陆军的正确解决方案。”

4、埃及出台首部网络安全法

新华网 8 月 21 日消息 据埃及官方媒体《埃及公报》报道，埃及总统塞西 8 月 18 日签署批准实施《反网络及信息技术犯罪法》，旨在打击极端分子利用互联网开展恐怖行动。这是埃及第一次在网络安全领域发布系统性法律，该法因此也有“首部网络安全法”之称。这部法律旨在打击非法使用计算机和信息网络的行为，保护政府及公共法人的数据、信息系统和网络免遭任何形式的攻击、渗透、篡改、毁损或破坏。比如，该法第一章规定“禁止未经许可将军队或警方的行动公布上网，禁止替恐怖主义的任何主张做宣传”。法律还要求对宪法保障的隐私进行保护，除非取得司法许可，任何人不得披露或窃听个人信息。针对各类型网络犯罪，该法细化了量刑的程度。例如，法律第七条允许监管部门在获得司法授权的情况下处罚或查封“威胁国家安全”或“制造虚假新闻”的网站，并对相关责任人实施监禁。第二十条规定，涉嫌非法侵入国家信息系统的个人将面临 5 万—20 万埃镑（1 元人民币约合 2.6 埃镑）的罚款，并可能被判处 2 年有期徒刑。法律还将冒用其他个人或机构之名注册电子邮箱、私人账号或网页的行为认定为犯罪，罪犯将面临 1 万至 3 万埃镑的罚款，情节严重者则将面临 3 个月监禁。这部法律规定，网络及通信服务供应商必须连续留存 180 天的详细系统记录，并有义务向相关政府监管机构提供特定用户及 IP 地址的数据信息，以应对网络犯罪和恐怖行动。《今日埃及报》《金字塔报》等当地主流媒体认为，该法律的出台有利于维护网络安全，提高网络监管的精细化法制化水平，维护社会稳定。

5、屈臣氏旗下英国知名药妆店 Superdrug 近 2 万名顾客个人信息遭泄露

根据英国媒体《每日邮报（DailyMail）》的报道，有黑客在本周一（8 月 20 日）晚上联系了屈臣氏集团（A.S. Watson）旗下英国知名药妆店 Superdrug，称他们已经获得了大约 2 万名 Superdrug 顾客的详细个人信息。作为证据，黑客还向 Superdrug 展示了 386 名 Superdrug 顾客的个人信息记录。经过 Superdrug 的确认，被黑客访问并且窃取的个人信息包括顾客的姓名、住址，以及部分顾客的出生日期、电话号码和积分余额。唯一值得庆幸的是，其中并不包括顾客的支付卡信息。Superdrug 坚称被黑客窃取的凭证是从入侵第三方得来的，而并非通过入侵 Superdrug 的系统。之所以能够进一步获取到 Superdrug 顾客的详细个人信息，这是因为黑客利用了人们有在各种在线服务使用相同密码的习惯。目前，我们还无法判定 Superdrug 这一说法的真实性。唯一可以肯定的是，Superdrug 顾客的个人信息的确已经遭到了泄露。黑客的目的极有可能是为了向 Superdrug 勒索赎金，但事实的真相还有待警方的调查。

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：高川

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158