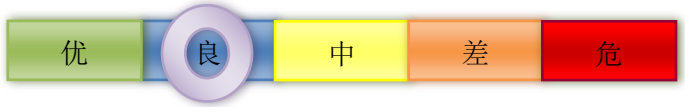
国家互联网应急中心

2018 年第 22 期

5 月 28 日-6 月 3 日

网络安全信息与动态周报

本周网络安全基本态势

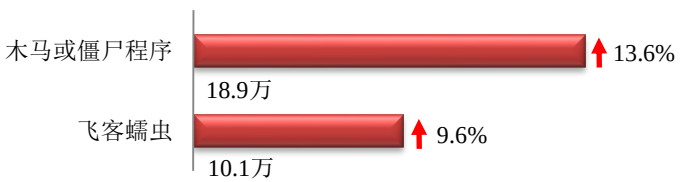


境内感染网络病毒的主机数量	•29.0万	↑ 12.2%
境内被篡改网站总数 其中政府网站数量	•912 •30	↓ 8.2% ↓ 3.2%
境内被植入后门网站总数 其中政府网站数量	•948 •29	↑ 15.0% ↓ 21.6%
针对境内网站的仿冒页面数量	•978	↓ 49.8%
新增信息安全漏洞数量 其中高危漏洞数量	•309 •127	↓ 7.8% ↑ 10.4%

═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

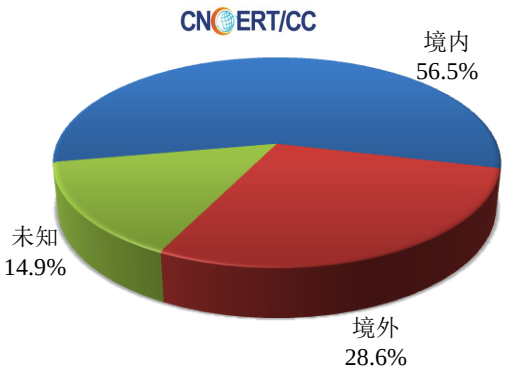
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 29.0 万个，其中包括境内被木马或被僵尸程序控制的主机约 18.9 万以及境内感染飞客（conficker）蠕虫的主机约 10.1 万。

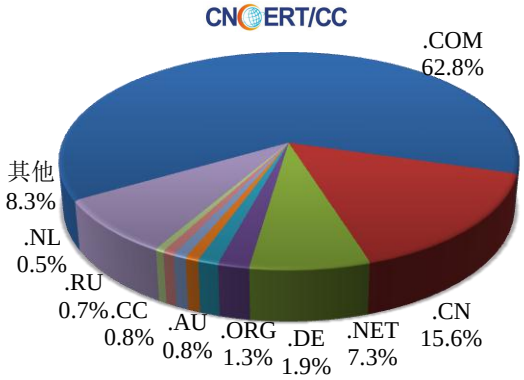


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1103 个，涉及 IP 地址 77356 个。在 1103 个域名中，有 28.6%为境外注册，且顶级域为.com 的约占 62.8%；在 77356 个 IP 中，有约 35.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 199 个 IP。

本周放马站点域名注册所属境内外分布
(5/28-6/3)



本周放马站点域名所属顶级域的分布
(5/28-6/3)



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。

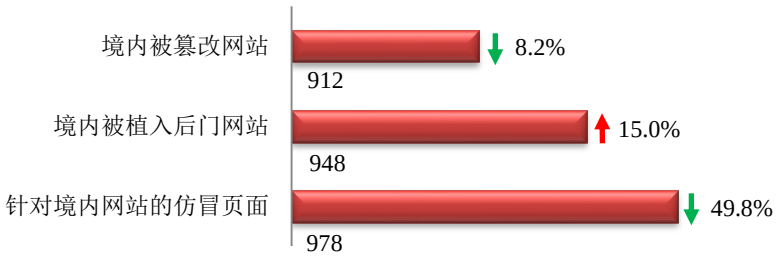
ANVA恶意地址黑名单发布地址

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。

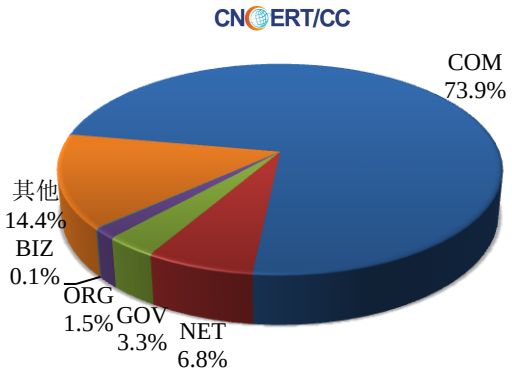
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 912 个；境内被植入后门的网站数量为 948 个；针对境内网站的仿冒页面数量为 978。

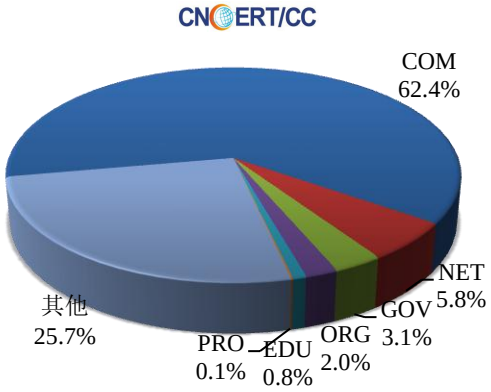


本周境内被篡改政府网站（GOV 类）数量为 30 个（约占境内 3.3%），较上周环比下降了 3.2%；境内被植入后门的政府网站（GOV 类）数量为 29 个（约占境内 3.1%），较上周环比下降了 21.6%；针对境内网站的仿冒页面涉及域名 412 个，IP 地址 185 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(5/28-6/3)

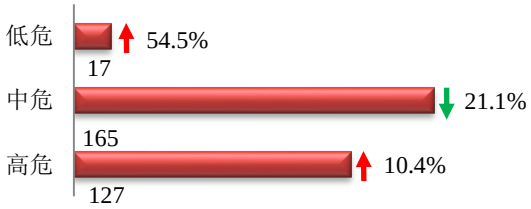


本周我国境内被植入后门网站按类型分布
(5/28-6/3)

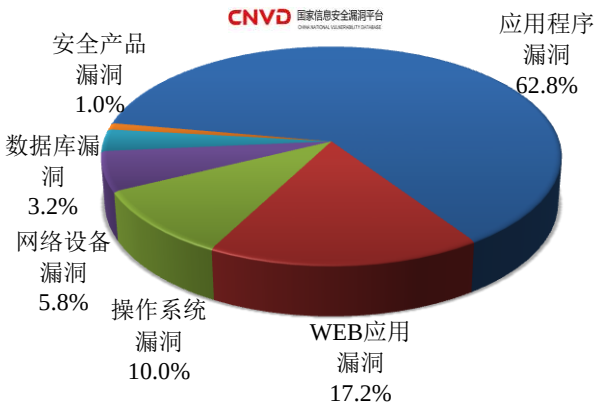


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 309 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
(5/28-6/3)



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

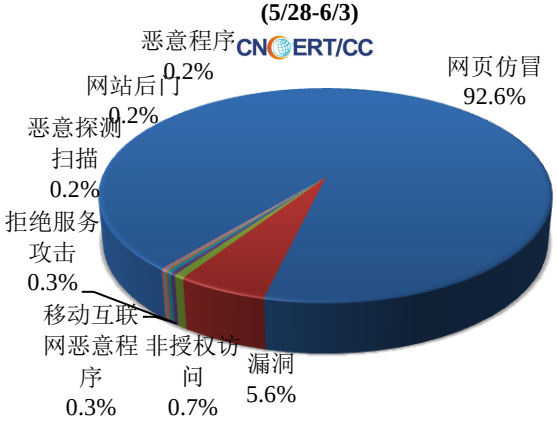
http://www.cnvd.org.cn/webinfo/list?type=4

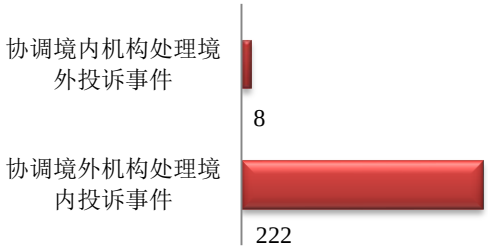
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 610 起，其中跨境网络安全事件 230 起。

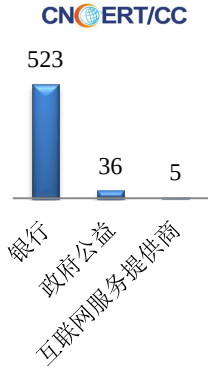
本周CNCERT处理的事件数量按类型分布 (5/28-6/3)



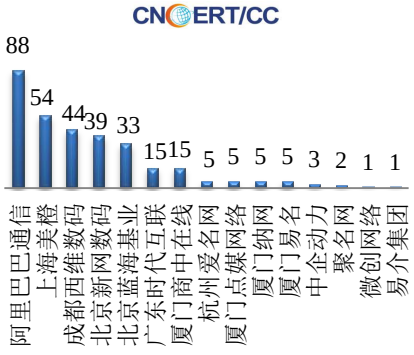


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 564 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 523 起和政府公益仿冒事件 36 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(5/28-6/3)



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 (5/28-6/3)



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 174 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
(5/28-6/3)

业界新闻速递

1、四部委发文加强核电运行安全管理

界面新闻 5 月 30 日消息 5 月 30 日，国家发改委、能源局、生态环境部、国防科工局联合印发《关于进一步加强核电运行安全管理的指导意见》，指导意见提出，核电运行安全始终处于受控状态，运行安全水平始终保持国际前列并持续提升。核电企业安全管理体系更加完善，安全生产责任制全面落实，安全管理水平持续提升。政府安全管理能力不断提高，核电行业安全管理、核安全监管、核应急响应、核安保能力进一步增强。核电安全得到更加充分、全面、有效的保障。

2、德国间谍机构被起诉，被指监控全球互联网交换数据

E 安全 6 月 1 日消息 当地时间 2018 年 5 月 30 日，德国东部城市莱比锡的联邦行政法院就德国商业互联网交换中心（De-Cix）质疑“德国联邦情报局（简称 BND）对该中心的数据流进行的全面监控”违反合法性一案进行了开庭审理。BND 还被认为与美国国家安全局（NSA）有合作。De-Cix 表示，其位于德国法兰克福的互联网交换中心是全球最大的互联网交换中心，涉及到来自中国、俄罗斯、中东和非洲的数据流，在流量高峰时每秒甚至处理 6TB 的数据。德国联邦情报局（BND）被指长期以来监听通过 De-Cix 交换的国际数据流。此外，De-Cix 认为，BND 获取德国国内通信的做法触犯了法律，并且表示有责任为保护客户做出努力，使 BND 对通信战略监控行为以合法方式进行。在当日的裁决中，德国法院驳回了 De-Cix 的控诉。De-Cix 正在考虑接下来是否向联邦宪法法院提出申诉。

3、加拿大两银行遭黑客侵袭 近 9 万名客户数据被窃

凤凰网 5 月 29 日消息 据路透社北京时间 5 月 29 日报道，加拿大蒙特利尔银行（Bank of Montreal）和加拿大帝国商业银行（Canadian Imperial Bank of Commerce）周一表示，网络攻击者可能窃取了两家银行近 9 万名

客户的数据，这似乎是该国金融机构首次遭到黑客重大攻击。加拿大第四大银行——蒙特利尔银行周一表示，网络黑客周日与该银行取得了联系，他们声称自己手上掌握了该银行 5 万客户的个人和财务信息。蒙特利尔银行表示，其认为发动此次攻击的黑客来自国外，该银行对导致客户数据被盗的风险敞口抱有信心，这些风险敞口目前已被封堵。加拿大第五大银行——加拿大帝国商业银行则表示，黑客周日联系了该银行，声称他们已通过电子方式窃取了其 Simplii direct banking 品牌下的 4 万名客户的个人和账户信息。加拿大帝国商业银行称，目前尚未证实黑客入侵了公司网络，但公司正在认真对待这一事件；该银行还称，旗下主要银行部门未受到影响。

4、伊朗机场电子显示屏遭黑客劫持

黑客视界 5 月 29 日消息 在上周四（5 月 24 日），位于伊朗东北部马什哈德市的机场遭到一群不明身份黑客的袭击。机场电子显示屏遭到黑客劫持，并向伊朗政府发出抗议宣言。据法尔达电台（Radio Farda）报道，黑客在机场出入口的电子显示屏上留下了一些图像，显示了一份抗议伊朗政府在中东地区军事存在的声明。声明以波斯语呈现，指责伊朗伊斯兰革命卫队（Islamic Revolutionary Guard Corps，IRGC）在黎巴嫩、叙利亚和加沙浪费伊朗人的生命和财政资源。这个自称 Tapandegan（Palpitaters）的黑客组织表示支持伊朗法尔斯省 Kazeroon 县居民的抗议活动，而这场抗议活动已经持续了长达数月的时间。报道指出，该组织之所以能够劫持电子显示屏并发布图像来源于他们成功侵入了马什哈德机场民用航空部负责人 Mohsen Eidizadeh 的电子邮箱。

5、比特币黄金遭黑客攻击：可能损失 1800 万美元

新浪网 5 月 28 日消息 北京时间 5 月 28 日早间消息，比特币黄金（Bitcoin Gold）的开发团队近期公布了上周遭遇攻击的详情。当时，攻击者通过“双重支出攻击”，从加密货币交易所中窃取了资金。比特币黄金的开发团队确认，攻击者获得了网络算力的大部分控制权，利用这些算力重组了比特币黄金的区块链，并进行反向交易。在这起事件中，攻击者向加密货币交易所存入资金，将其交易为比特币或其他加密货币，随后再提取资金。随后，攻击者使用获得的绝大部分算力，迫使网络的其他部分接受伪造的数据块，修改最初的存入资金，导致这些资金从交易所控制的钱包中消失。根据此前的报道，与攻击者关联的地址在一系列“双重支出行为”的交易中向自己发送了超过 38 万个比特币黄金。目前尚不清楚，这些交易中有多少造成了资金被盗。从理论上来说，如果所有交易都造成资金被盗，那么攻击者可以从中获利 1800 万美元。

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：徐剑

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158