国家互联网应急中心

网络安全信息与动态周报

2019 年第 26 期

6 月 24 日-6 月 30 日

CNCERT/CC

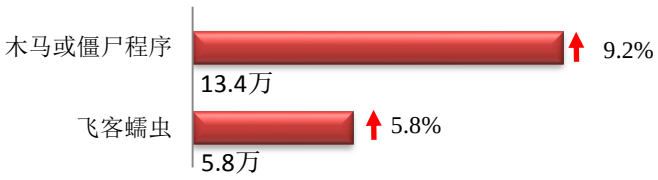
本周网络安全基本态势

境内感染网络病毒的主机数量	• 19.1万	↑ 8.1%
境内被植入后门网站总数 其中政府网站数量	• 3454 • 62	↑ 6.0% ↑ 29.2%
新增信息安全漏洞数量 其中高危漏洞数量	• 201 • 72	↑ 0.5% ↑ 44.0%

= 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

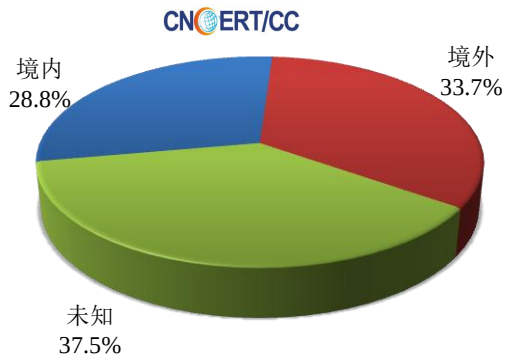
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 19.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 13.4 万以及境内感染飞客（conficker）蠕虫的主机约 5.8 万。

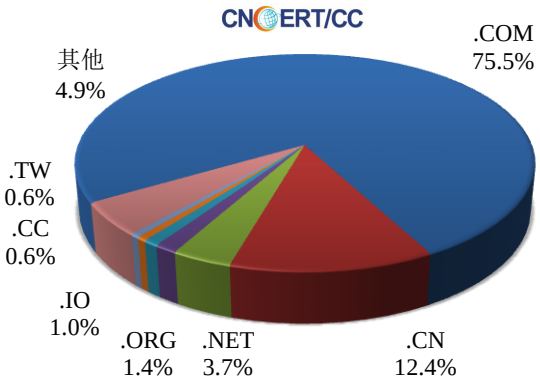


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 7776 个，涉及 IP 地址 4059 个。在 7776 个域名中，有 33.7%为境外注册，且顶级域为.com 的约占 75.5%；在 4059 个 IP 中，有约 55.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 525 个 IP。

本周放马站点域名注册所属境内外分布
(6/24-6/30)



本周放马站点域名所属顶级域的分布
(6/24-6/30)



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

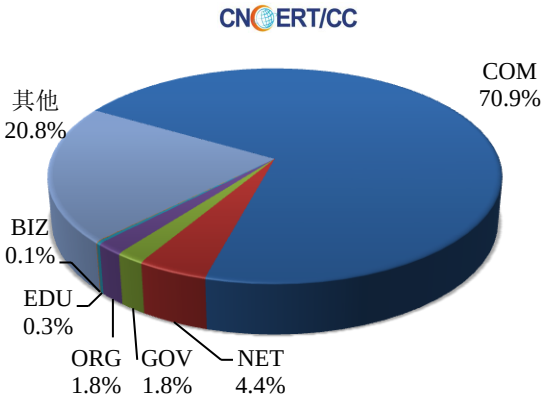
中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由中国互联网协会网络与信息安全工作委员会发起、CNCERT 具体组织运作的行业联盟。

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 3259 个。

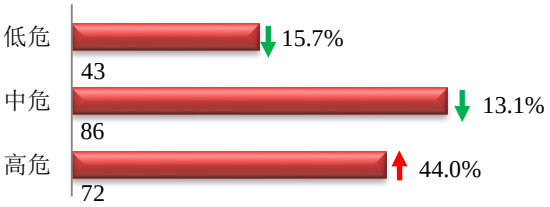
境内被植入后门的政府网站（GOV 类）数量为 62 个（约占境内 1.8%），较上周环比下降上升 29.2%；针对境内网站的仿冒页面涉及域名 569 个，IP 地址 289 个，平均每个 IP 地址承载了约 7 个仿冒页面。

本周我国境内被植入后门网站按类型分布
(6/24-6/30)

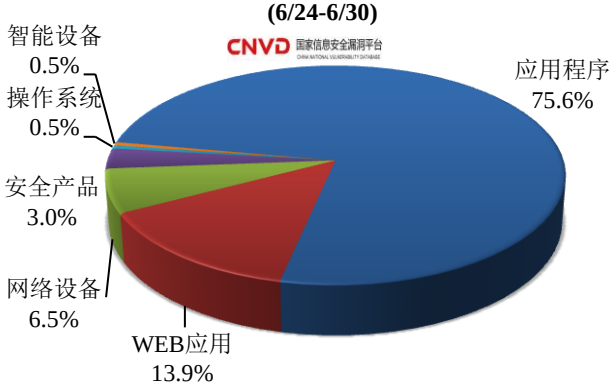


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 201 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
(6/24-6/30)



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

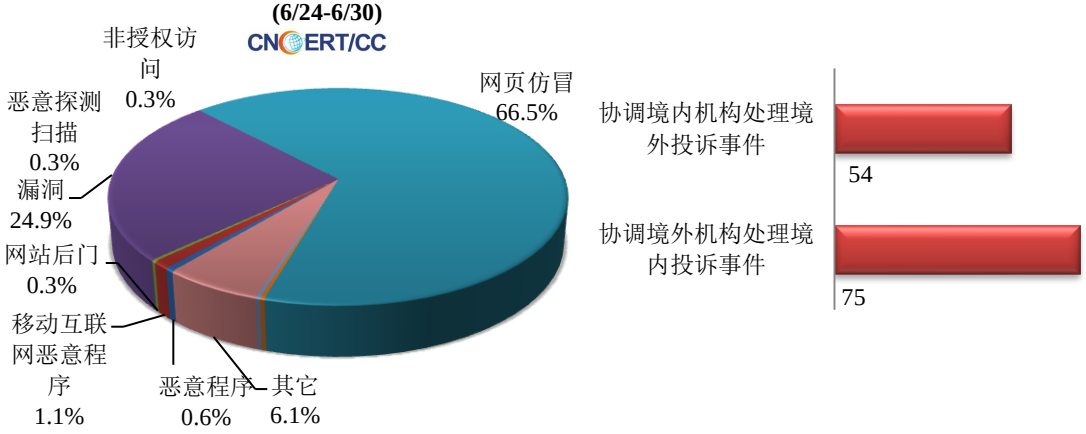
http://www.cnvd.org.cn/webinfo/list?type=4

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 361 起，其中跨境网络安全事件 129 起。

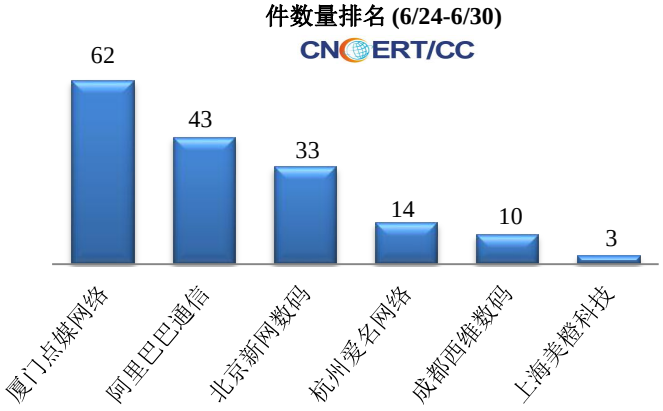
本周CNCERT处理的事件数量按类型分布 (6/24-6/30)



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 240 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 237 起和证券仿冒事件 2 起。

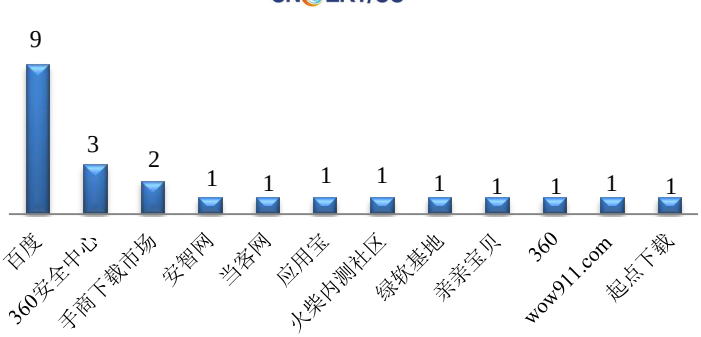
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (6/24-6/30)

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 (6/24-6/30)



本周，CNCERT 协调 12 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 23 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
(6/24-6/30)



业界新闻速递

1、 密码法草案首次亮相 明确密码分类管理原则

新京报 6 月 25 日消息 十三届全国人大常委会第十一次会议初次审议密码法草案，草案提出，密码分为核心密码、普通密码和商用密码，实行分类管理；特定范围的商用密码实行进口许可和出口管制。草案共五章四十四条，其中提出了密码分类保护的原则要求：核心密码、普通密码用于保护国家秘密信息，核心密码保护信息的最高密级为绝密级，普通密码保护信息的最高密级为机密级；核心密码、普通密码属于国家秘密，由密码管理部门依法实行严格统一管理。商用密码用于保护不属于国家秘密的信息；公民、法人和其他组织均可依法使用商用密码保护网络与信息安全。

2、 工信部同意中国互联网络信息中心设立域名根服务器及运行机构

工信部官网 6 月 26 日消息 工业和信息化部日前批复同意中国互联网络信息中心设立域名根服务器（F、I、K、L 根镜像服务器）及域名根服务器运行机构，同意该中心负责运行、维护和管理编号分别为 JX0001F、JX0002F、JX0003I、JX0004K、JX0005L、JX0006L 的域名根服务器，并要求其严格遵守《互联网域名管理办法》《通信网络安全防护管理办法》及相关法律法规、行政规章及行业管理规定，接受工信部的管理和监督检查，保证域名根服务器安全、可靠运行。

3、 瘫痪 2 周后 美国又一城市宣布向黑客支付价值将近 50 万美元的赎金

Cnbeta.COM6 月 27 日消息 在美国佛州 Riviera City 成为首个同意向黑客支付赎金（高达 60 万美元）的城市之后，佛州又有一个城市宣布采取相同的应对方式。莱克城（Lake City）位于佛州北部，拥有 6.5 万人口，在本次黑客攻击中各项市政工作已经停摆两周时间。在周一的市政紧急会议中，通过投票决定支付 42 个比特币，价值将近 50 万美元的赎金。在感染后一周莱克城就收到了赎金请求，并且通过保险提供商 League of Cities 进行谈判，确认了 42 个比特币的赎金。

4、 荷兰突发重大电信中断事故

E 安全 6 月 25 日消息荷兰皇家电信公司（Royal KPN NV）网络中断，停电持续了数小时，同时也影响了使用 KPN 骨干网的其他电信运营商。这次停电开始于当地时间 16:00（格林尼治时间 14:00）之前，是荷兰历史上最大的一次停电事故。国家安全与反恐协调发言人表示，目前首要任务是确保一切恢复正常。

5、 研究发现黑客已渗透十多家运营商 必要时可切断通讯网络

Cnbeta.COM6 月 25 日消息 根据总部位于波士顿的安全公司 Cybereason 近期发布的安全警告，在过去七年中黑客一直利用已经渗透的运营商网络来窃取敏感数据，甚至于在必要的时候可以完全关闭通讯网络。安全研究人员表示，他们一直在调查名为 Operation Softcell 的黑客活动，攻击目标主要针对欧洲、亚洲、非洲和中东地区的移动运营商。自 2012 年开始不断有移动运营商被悄然渗透，获取完整的网络控制权限，并吸取了数百 GB 的用户数据。这些黑客拥有所有用户名和密码，并为自己创建了一系列特权，能够做任何他们想要做的事情。黑客拥有高级别的访问权限，甚至可以关闭整个通讯网络。

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：雷君

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315