国家互联网应急中心

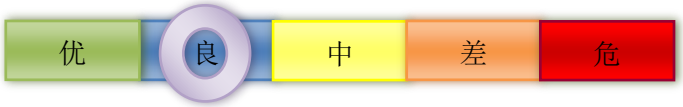
网络安全信息与动态周报

2018 年第 27 期

7 月 2 日-7 月 8 日

CNCERT/CC

本周网络安全基本态势

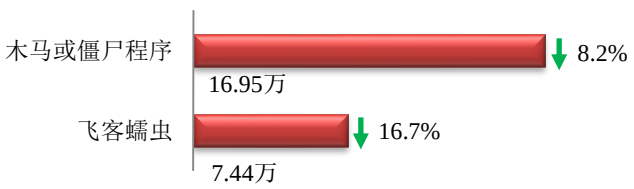


境内感染网络病毒的主机数量	•24.39万	↓ 10.9%
境内被篡改网站总数 其中政府网站数量	•917 •32	↑ 14.2% ↑ 6.7%
境内被植入后门网站总数 其中政府网站数量	•908 •15	↑ 17.3% =
针对境内网站的仿冒页面数量	•1016	↓ 13.1%
新增信息安全漏洞数量 其中高危漏洞数量	•179 •55	↓ 37.2% ↓ 48.6%

=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

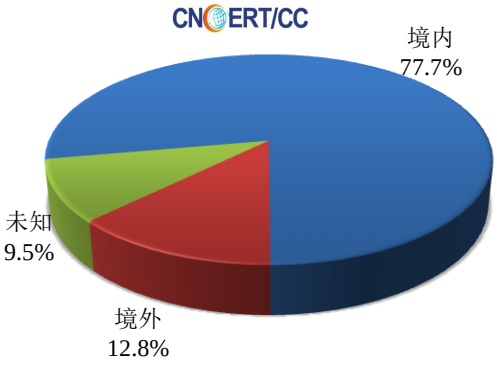
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 24.39 万个，其中包括境内被木马或被僵尸程序控制的主机约 16.95 万以及境内感染飞客（conficker）蠕虫的主机约 7.44 万。

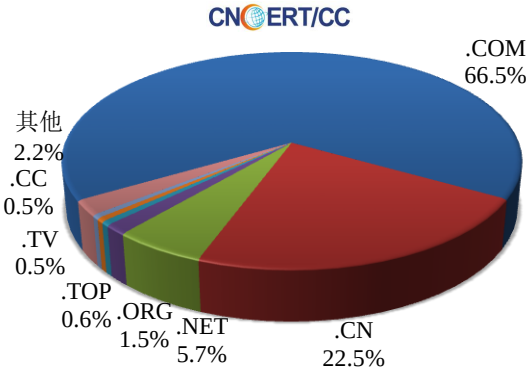


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1904 个，涉及 IP 地址 100753 个。在 1904 个域名中，有 12.8%为境外注册，且顶级域为.com 的约占 66.5%；在 100753 个 IP 中，有约 31.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 212 个 IP。

本周放马站点域名注册所属境内外分布
(7/2-7/8)



本周放马站点域名所属顶级域的分布
(7/2-7/8)



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。

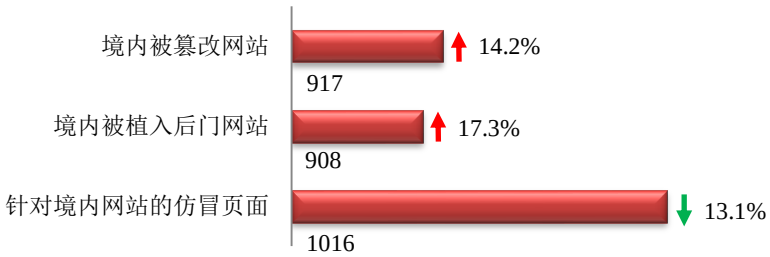
ANVA恶意地址黑名单发布地址

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。

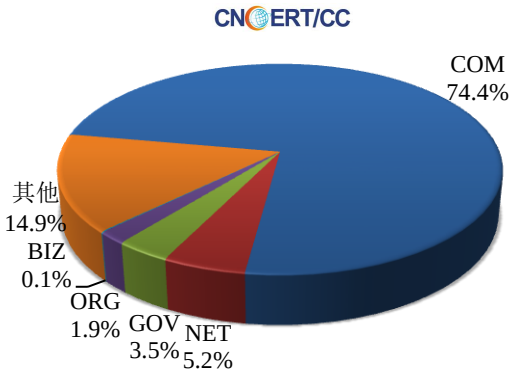
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 917 个；境内被植入后门的网站数量为 908 个；针对境内网站的仿冒页面数量为 1016。

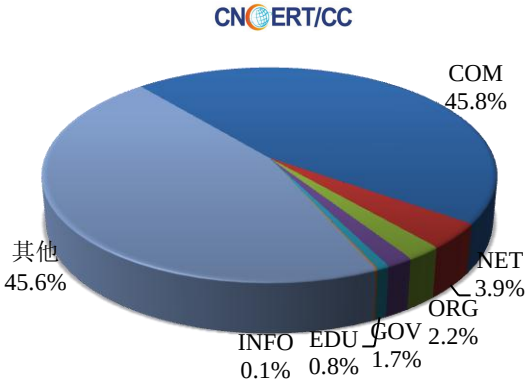


本周境内被篡改政府网站（GOV 类）数量为 32 个（约占境内 3.5%），较上周环比上升了 6.7%；境内被植入后门的政府网站（GOV 类）数量为 15 个（约占境内 1.7%），较上周持平；针对境内网站的仿冒页面涉及域名 410 个，IP 地址 218 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(7/2-7/8)

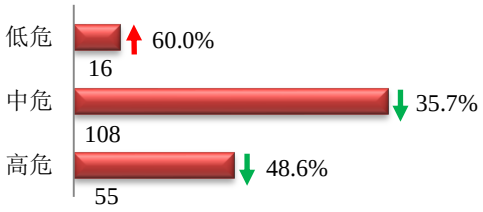


本周我国境内被植入后门网站按类型分布
(7/2-7/8)

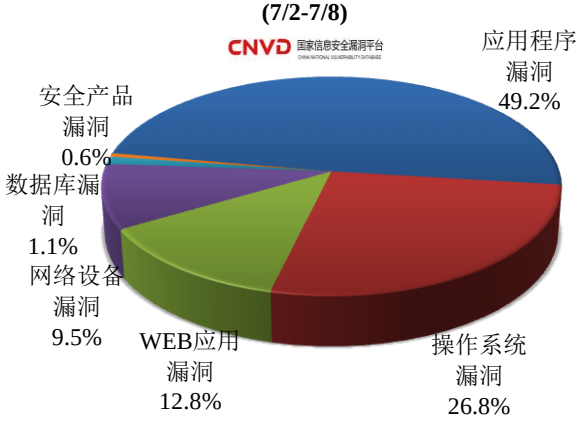


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 179 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
(7/2-7/8)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是操作系统漏洞和 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

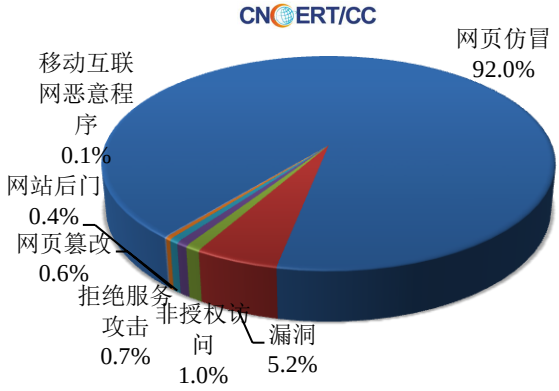
http://www.cnvd.org.cn/webinfo/list?type=4

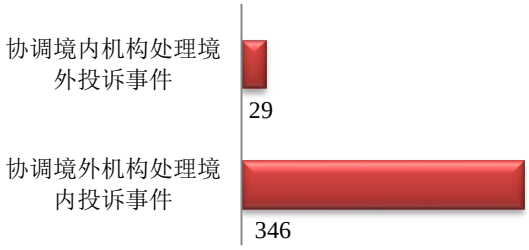
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 829 起，其中跨境网络安全事件 375 起。

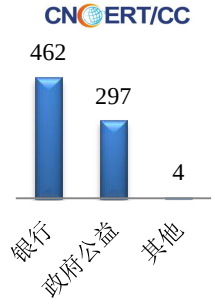
本周CNCERT处理的事件数量按类型分布 (7/2-7/8)



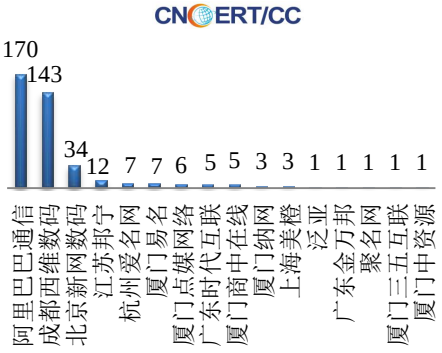


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 763 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 462 起和政府公益仿冒事件 297 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(7/2-7/8)

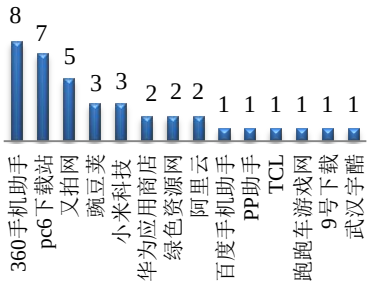


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (7/2-7/8)



本周，CNCERT 协调 14 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 38 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
(7/2-7/8)



业界新闻速递

1、白宫政府机构改革计划：网络安全队伍建设

E 安全 7 月 3 日消息 近日，美国白宫发布一份联邦政府机构改革计划，希望减少机构职能重叠、提升工作效率，欲制定统一的战略以加强政府各部门的网络安全队伍建设。这份改革计划指出，美国政府各机构在任务交付、客户服务和税收管理方面存在相互联系的必要性。出于对美国政府机构重组进行更广泛的系统层面思考，美国需要解决网络安全与网络战、数字服务交付与 IT 现代化、有效利用数据进行问责和透明度管理这三个领域变革所面临的互联障碍。

2、白宫或将启动全球 APT 黑客组织全面调查

E 安全 7 月 4 日消息 美国众议院外交事务委员会 2018 年 6 月 28 日通过“2018 网络威慑与响应法案”（H. R. 5576），要求美国总统确认高级持续威胁（APT）组织名单，并在《联邦公报》（Federal Register）中公布并定期更新。该法案还要求美国政府制裁对美国发动国家支持型网络攻击的参与者。从广义上讲，该法案寻求制定一项战略，允许美国采取行动响应外国黑客发起的攻击。该法案将调整政策，并就美国联邦行政机构如何增加对手的成本（对美国企业或政府机构发起网络攻击）制定新的控制措施。该法案要求，美国总统提供一份全面的外国黑客组织名单，便于美国政府机构讨论特定网络威胁时使用通用的名称指代。该法案的措辞表明，名单将不包含与美国有关或可能与其盟友有关的黑客组织，名单仅包含美国认为对其构成重大威胁的黑客或黑客组织。法案提出了多项制裁举措，包括安全保障、非人道主义援助、禁止国际贷款和金融协议、禁止财务转账、禁止赴美旅游、限制在美投资或开展业务，以及限制美国公司向这些人销售产品或技术。

3、俄罗斯军方将利用区块链追踪黑客攻击来源

BiaNews7 月 2 日消息 2018 年 7 月 2 日，俄罗斯联邦国防部正在时代科技园设立一个独特的研究实验室，

区块链技术将被开发应用于加强网络安全，打击对关键信息基础设施的网络攻击。根据卡巴斯基实验室反病毒专家 Alexey Malanov 认为，区块链将有助于军方追踪黑客攻击的来源，并提高数据库的总体安全性。Alexey Malanov 表示，非法侵入者通常会清理权限日志，以隐藏非法访问设备的痕迹。但是，如果日志分布在多个设备之间（例如，通过区块链技术），那么这种风险可以最小化。区块链是一种创新的、有用的技术，可以在商业和军队中成功应用。病毒改变数据或软件代码，并试图掩盖它从数据完整性控制器。同时区块链可以存储参考码，确保独立验证和数据/代码的有效性。除了用于传输密码信息的专用网络之外，国防部还拥有可上网的系统和设备。铁道部的各个行政部门都将其用于会计和工作流管理，这使得它们很容易受到黑客攻击。

4、Facebook 承认允许 61 家公司访问用户数据

凤凰网 7 月 2 日消息 据 CNBC 北京时间 7 月 2 日报道，Facebook 承认，即使在 2015 年宣布限制对此类数据的访问后，它仍然允许 61 家公司访问用户数据。《华尔街日报》刊文称，当地时间上周五，Facebook 向美国国会提交了 747 页文档。Facebook 在文档中承认，它“一次性”给予 AOL、耐克、UPS 和约会应用 Hinge 等公司 6 个月时间，使它们有时间适应公司在用户数据方面政策的修改。Facebook 称，另外，至少其他 5 家公司可能访问了有限的用户数据，原因是 Facebook 在一次试验中授予了它们数据访问权限。Facebook 2015 年宣称已经禁止开发者访问其用户以及用户好友的数据。

5、PowerShell 发生多起攻击案例，目标多瞄准数字货币

BiaNews7 月 3 日消息 近期，利用 PowerShell 执行恶意代码的攻击频繁发生。此类型攻击利用受害者系统正常应用白进程调用同名资源文件来执行恶意代码，从而绕过安全软件的拦截，使受害者难以发现。据悉，通过 PowerShell 下载读取云端图片，图片内藏恶意编码的 Shellcode 代码和攻击模块，恶意模块被加载后会默认安装恶意浏览器插件进一步实施挖矿，劫持用户数字货币交易行为。倘若该中毒电脑上进行数字虚拟货币交易，木马可以在交易瞬间将收款人钱包地址换成病毒设定的钱包地址，成功实现抢钱目的。

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：贾子骁

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158