国家互联网应急中心

网络安全信息与动态周报

2018 年第 23 期

6 月 4 日-6 月 10 日

CNCERT/CC

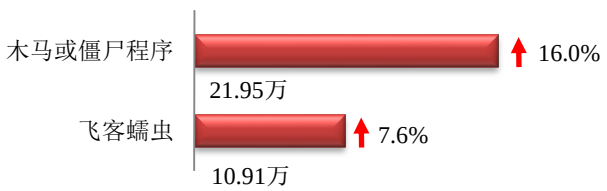
本周网络安全基本态势

境内感染网络病毒的主机数量	•32.86万	↑ 13.1%
境内被篡改网站总数 其中政府网站数量	•1040 •30	↑ 14.0% =
境内被植入后门网站总数 其中政府网站数量	•974 •22	↑ 2.7% ↓ 24.1%
针对境内网站的仿冒页面数量	•1077	↑ 10.1%
新增信息安全漏洞数量 其中高危漏洞数量	•212 •70	↓ 31.4% ↓ 44.9%

=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

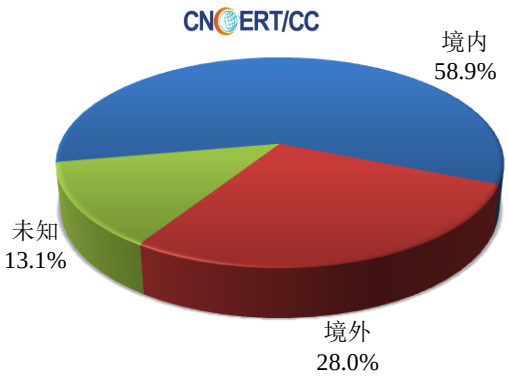
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 32.86 万个，其中包括境内被木马或被僵尸程序控制的主机约 21.95 万以及境内感染飞客（conficker）蠕虫的主机约 10.91 万。

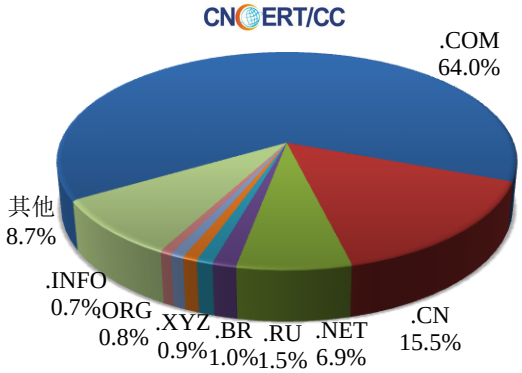


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1099 个，涉及 IP 地址 74572 个。在 1099 个域名中，有 28.0%为境外注册，且顶级域为.com 的约占 64.0%；在 74572 个 IP 中，有约 35.0%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 246 个 IP。

本周放马站点域名注册所属境内外分布
(6/4-6/10)



本周放马站点域名所属顶级域的分布
(6/4-6/10)



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。

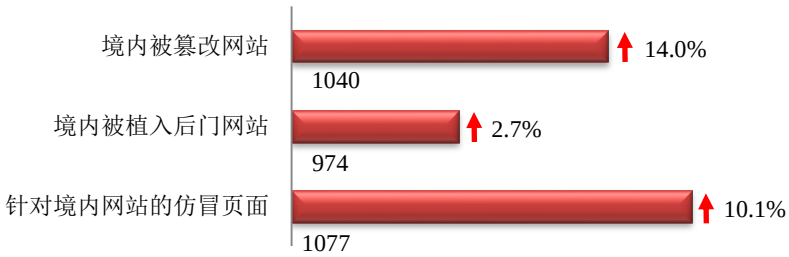
ANVA恶意地址黑名单发布地址

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。

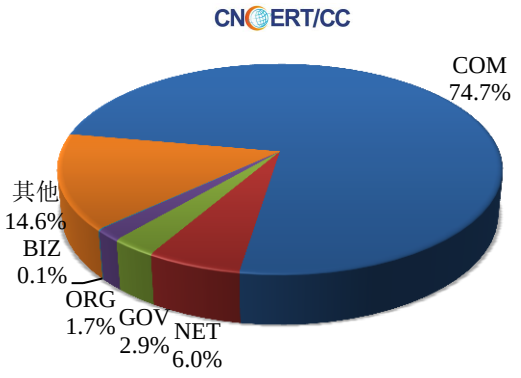
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1040 个；境内被植入后门的网站数量为 974 个；针对境内网站的仿冒页面数量为 1077。

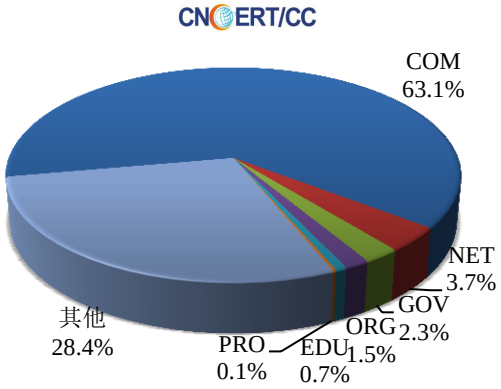


本周境内被篡改政府网站（GOV 类）数量为 30 个（约占境内 2.9%），与上周持平；境内被植入后门的政府网站（GOV 类）数量为 22 个（约占境内 2.3%），较上周环比下降了 24.1%；针对境内网站的仿冒页面涉及域名 428 个，IP 地址 181 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(6/4-6/10)

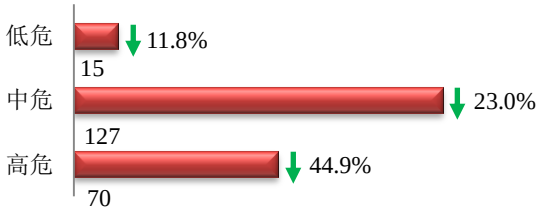


本周我国境内被植入后门网站按类型分布
(6/4-6/10)

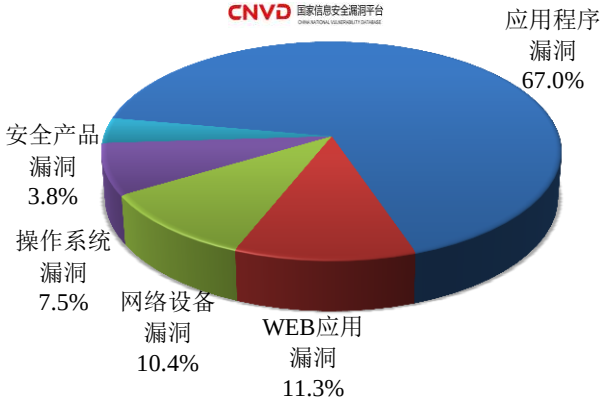


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 212 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
(6/4-6/10)



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

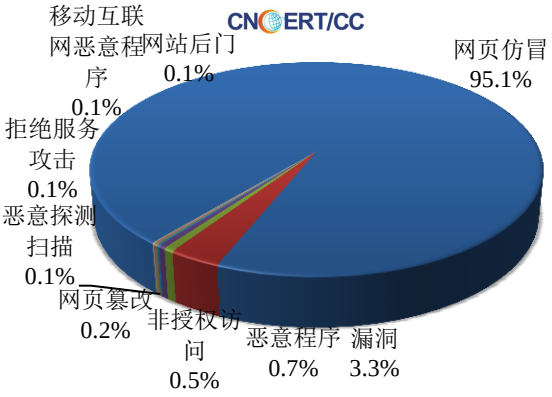
http://www.cnvd.org.cn/webinfo/list?type=4

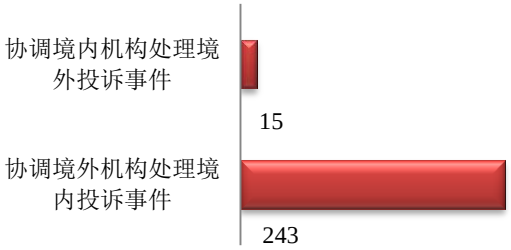
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 1071 起，其中跨境网络安全事件 258 起。

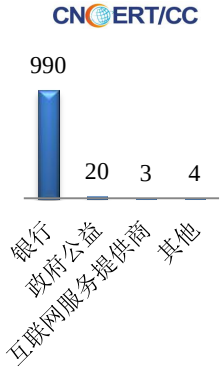
本周CNCERT处理的事件数量按类型分布 (6/4-6/10)



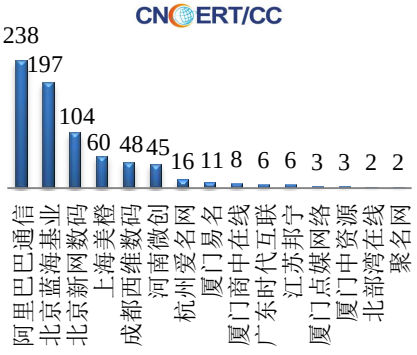


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1017 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 990 起和政府公益仿冒事件 20 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(6/4-6/10)



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 (6/4-6/10)



本周，CNCERT 协调 8 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 33 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
(6/4-6/10)

业界新闻速递

1、美将利用“五眼联盟”信息共享计划抵御俄罗斯黑客攻击

E 安全 6 月 4 日消息 美国众议院首席信息安全官兰迪·维克斯透露，美国众议院正在试图扩大与“五眼联盟”成员国议会的网络威胁信息共享计划，以加强这些国家最高立法机关（国会或议会）的安全性。共享的信息可能是指非保密性威胁情报。维克斯表示，“五眼联盟”的最高立法机关已经维系了牢固的信息共享关系，但美国众议院的目标是能更充分地利用这种关系，且目前正在研究如何更有效、更频繁地共享信息，但需确保“五眼联盟”达成共识，以充分了解网络威胁形势。这项计划的实现方式可能很简单，比如由美国国土安全部（DHS）向“五眼联盟”成员国发出网络安全公告，各成员国可通过威胁情报平台了解相关信息。

2、美智库报告：提出多项增强各州政府网络安全建议

E 安全 6 月 6 日消息 美国智库新美国基金会（New America Foundation）的网络安全倡议项目于 2018 年 5 月 31 日发布报告，建议联邦政府考虑三项“优先努力”，以帮助各州政府推进改善其网络安全。包括：一、建议联邦政府指定与国家优先事项相关的特别网络安全资金。报告称，这种资助机制可以为各州和地方的政策制定者提供指导，并有助于简化国家生态系统。二、建议联邦政府采取措施缓解和简化联邦事件的响应、指导和援助项目。报告称，目前的“烟囱结构”在许多领域（如时间报告和监管要求方面）制定了相互矛盾的指导方针。三、建议联邦政府优先考虑和扩大正式的本地化援助计划，尤其是国土安全部（DHS）和国防部（DoD）。报告表示，美国各州、地方、部落和地区在网络安全方面的努力很大程度上依赖个人关系，因此当前全国范围内所存在的相关项目大都存在资源不足或不够成熟的问题。此外，该智库在撰写这一报告时，认真考察了美国各州为推进网络安全工作所做的努力，并在报告中指出了值得学习和借鉴的经验教训，包括与私营部门建立信任关系；在法律或行政命令中明确角色、职责和权力；签署跨机构的协议或建立跨机构的结构。

3、Facebook 被曝常年向苹果等 60 家手机厂提供用户隐私

HackerNews.cc6 月 4 日消息 社交网络巨头 Facebook 陷入了公司历史上史无前例的舆论抨击风暴中，原因是向外界擅自披露用户数据和信息，侵犯民众隐私权益。Facebook 的丑闻并未结束，据美国媒体最新爆料，多年来，Facebook 向全球大批手机厂商提供了用户信息，包括私人日程安排等，最近批评 Facebook 的苹果公司也是获得信息的厂商之一。Facebook 旗下拥有 20 亿用户，该公司长期倡导实名制，但是 Facebook 对外散布用户信息的举动，却达到了触目惊心的地步。据美国《纽约时报》6 月 3 日披露，在过去多年中，Facebook 一共和大约 60 家设备厂商签署了协议，向他们提供用户隐私信息，这些厂商中包括了三星、苹果、微软、黑莓、亚马逊等。

4、DNA 检测公司 MyHeritage 遭黑客入侵：9200 万账户泄露

新浪网 6 月 6 日消息 北京时间 6 月 6 日早间消息，消费级家谱网站 MyHeritage 宣布，与该公司的 9200 万个帐户相关的电子邮件地址和密码信息被黑客窃取。MyHeritage 表示，该公司的安全管理员收到一位研究人员发送的消息，后者在该公司外部的一个私有服务器上发现了一份名为《myheritage》的文件，里面包含了 9228 万个 MyHeritage 帐号的电子邮件地址和加密密码。据 Heritage 介绍，该漏洞发生在 2017 年 10 月 26 日，受影响的用户都是在那一天之前注册的。该公司还表示，他们并没有存储用户的密码，所有密码都经过所谓的单项散列方式进行加密，不同用户的数据需要使用不同的密钥才能访问。但在之前的黑客事件中，这类机制曾经遭到破解，从而转换出密码。倘若如此，黑客便可获在登录用户帐号后获取其个人信息，包括家庭成员的身份。但即使黑客能够进入用户帐号，也不太可能轻易获取原始基因信息，因为想要下载这些内容，需要通过电子邮件进行确认。

5、HR 软件公司 PageUp 遭恶意软件感染 超过 200 万用户个人信息或已泄露

黑客视界 6 月 7 日消息 据外媒 ZDNet 报道，总部位于澳大利亚的人力资源（Human Resource，HR）软件公司 PageUp 已经证实，它的 IT 基础设施在上个月被发现存在异常活动，这可能会导致客户数据的泄露。5 月 23 日，在发现系统感染恶意软件之后，该公司立即展开了深入调查。经过 5 天的调查，该公司表示其担心得到了证实，调查结果中的一些指标表明某些客户数据极有可能已经遭到泄露。澳大利亚电信服务提供商 Telstra 也就 PageUp 事件发表了声明，称在大多数情况下，可能受到影响的个人信息是申请人的姓名、电话号码、申请历史和电子邮箱地址。而对于那些申请成功的人来说，PageUp 系统中的数据可能包括：出生日期、就业机会细节、员工编号（如果是现任或前任员工）、就业前检查结果和仲裁细节。PageUp 公司最后还表示，它已就此事与澳大利亚网络安全中心（ACSC）、澳大利亚计算机应急响应小组（CERT）、澳大利亚信息专员办公室（OAIC）以及英国国家网络安全中心（NCSC）进行了联系，并建议用户更改自己的密码。

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：王适文

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158