国家互联网应急中心

2018 年第 24 期

6 月 11 日-6 月 17 日

网络安全信息与动态周报

本周网络安全基本态势

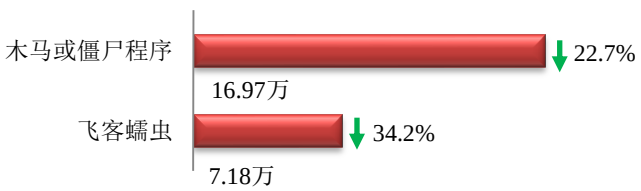
优 | 良 | 中 | 差 | 危

境内感染网络病毒的主机数量	•24.15万	↓ 26.5%
境内被篡改网站总数 其中政府网站数量	•1131 •30	↑ 8.7% =
境内被植入后门网站总数 其中政府网站数量	•732 •16	↓ 24.8% ↓ 27.3%
针对境内网站的仿冒页面数量	•937	↓ 13.0%
新增信息安全漏洞数量 其中高危漏洞数量	•302 •109	↑ 42.5% ↑ 55.7%

=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

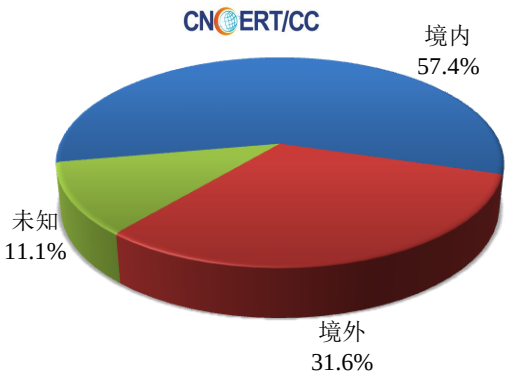
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 24.15 万个，其中包括境内被木马或被僵尸程序控制的主机约 16.97 万以及境内感染飞客（conficker）蠕虫的主机约 7.18 万。

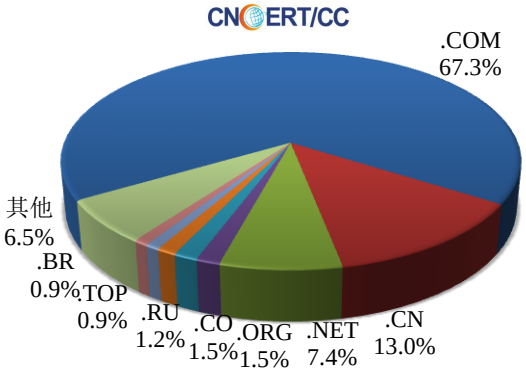


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 678 个，涉及 IP 地址 57611 个。在 678 个域名中，有 31.6%为境外注册，且顶级域为.com 的约占 67.3%；在 57611 个 IP 中，有约 31.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 178 个 IP。

本周放马站点域名注册所属境内外分布
(6/11-6/17)



本周放马站点域名所属顶级域的分布
(6/11-6/17)



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。

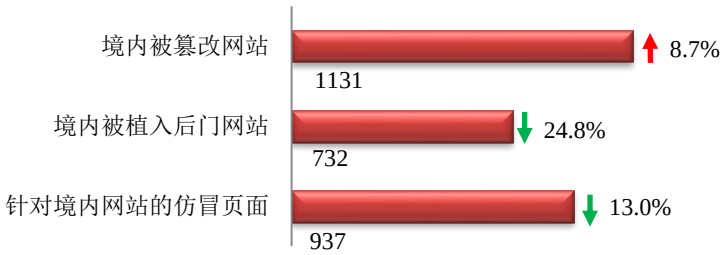
ANVA恶意地址黑名单发布地址

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。

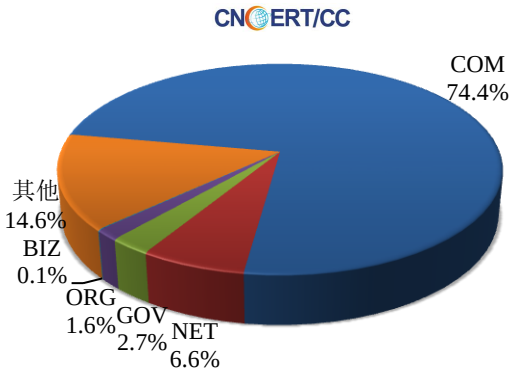
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1131 个；境内被植入后门的网站数量为 732 个；针对境内网站的仿冒页面数量为 937。

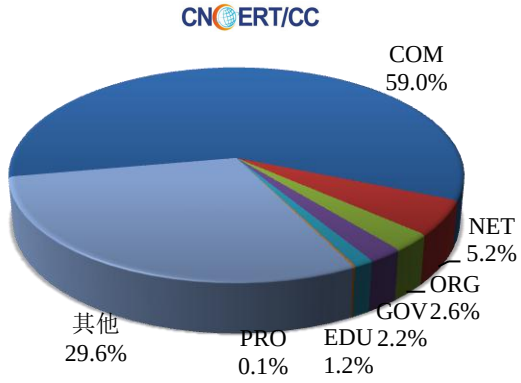


本周境内被篡改政府网站（GOV 类）数量为 30 个（约占境内 2.7%），与上周持平；境内被植入后门的政府网站（GOV 类）数量为 16 个（约占境内 2.2%），较上周环比下降了 27.3%；针对境内网站的仿冒页面涉及域名 376 个，IP 地址 208 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(6/11-6/17)

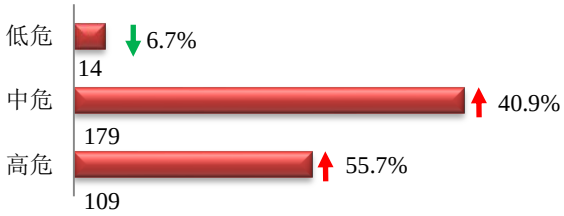


本周我国境内被植入后门网站按类型分布
(6/11-6/17)

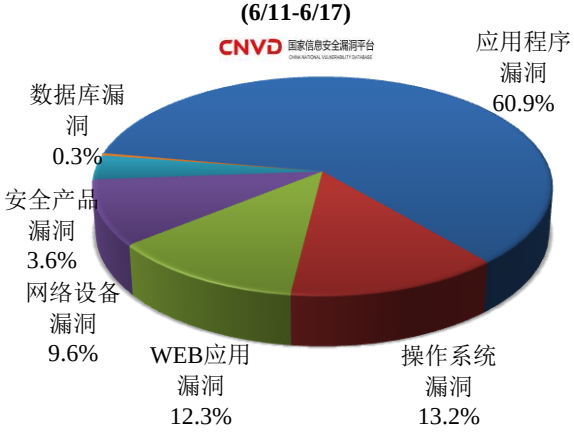


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 302 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
(6/11-6/17)



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

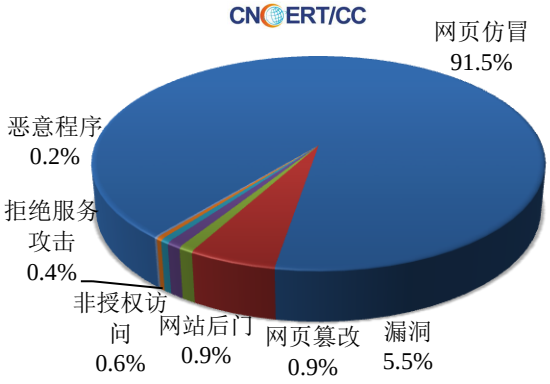
http://www.cnvd.org.cn/webinfo/list?type=4

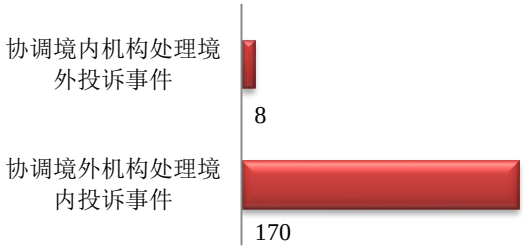
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 532 起，其中跨境网络安全事件 178 起。

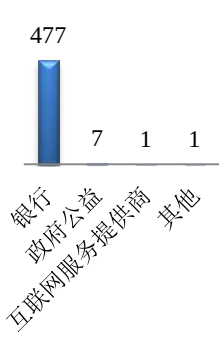
本周CNCERT处理的事件数量按类型分布 (6/11-6/17)



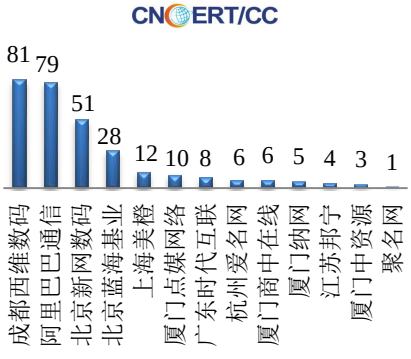


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 486 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 477 起和政府公益仿冒事件 7 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(6/11-6/17)

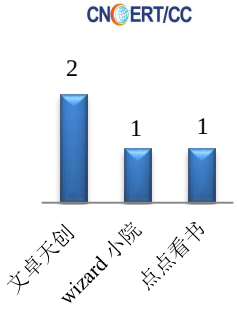


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (6/11-6/17)



本周，CNCERT 协调 3 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 4 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
(6/11-6/17)



业界新闻速递

1、美众议院委员会通过保护关键基础设施第 5733 号法案

E 安全 6 月 11 日消息 美国众议院国土安全委员会于当地时间 2018 年 6 月 6 日对多项法案进行审议，并通过了第 5733 号法案。第 5733 号法案提出对《2002 年国土安全法》进行修订，要求美国国土安全部（DHS）下的国家网络安全和通信整合中心（NCCIC）识别并应对关键基础设施自动化控制过程中所用产品和技术的漏洞和威胁。第 5733 号法案要求，NCCIC 需向制造商、终端用户和行业利益相关者提供技术支持，以识别并缓解可能影响这些关键系统的漏洞。此外，NCCIC 还需提供其它保障措施，以保护美国的关键行业，包括电力和供水系统、制造业、交通运输、能源等。此外，NCCIC 还必须在此法案颁布后 180 天内，以及在这之后的四年间，每 6 个月要向美国众议院国土安全委员会、参议院国土安全和政府事务委员会报告其在保护工业控制系统方面采取的举措。

2、美国以策划秘密网络攻击为由对部分俄实体施加制裁

环球网 6 月 12 日消息 据英国路透社 6 月 12 日报道，美国财政部在 11 日对三名俄罗斯人和五家公司实施了制裁，称他们与俄罗斯军方和情报部门合作，研究如何对美国及其盟友实施网络攻击。美国财政部长史蒂芬•努钦在一份报告中表示：“美国正在开展一项持续努力，打击俄罗斯联邦及其军事和情报部门的恶意行为，以增强抵御俄罗斯网络攻击的能力。”努钦说：“今天被指认的俄罗斯实体过去曾与俄罗斯联邦安全局（FSB）合作，为提高俄罗斯的网络攻击能力和水下侦查能力做了很多，进而危及了美国及盟友的安全。”这些指认意味着目标实体所有的属美国管辖范围内的房地产都将接受限制，并禁止美国公民与其有交易。

3、欧盟将建通用网络安全认证框架

E 安全 6 月 12 日消息 欧盟将针对信息和通信技术（ICT）产品、服务和流程建立一个欧盟范围内的认证框

架，以此加强网络弹性。ICT 行业可利用这种新机制认证联网汽车、智能医疗设备等产品。2018 年 6 月 8 日在卢森堡举行的会议上，欧盟委员会的电信委员会就网络安全法草案达成“总体方针”。这项法律草案提出创建机制，为特定的信息和通信技术（ICT）流程、产品和服务建立欧盟网络安全认证框架。按照计划，签发的证书将在所有欧盟国家有效，其更易使用户对这些技术的安全性抱有信心，并促进企业跨境开展业务。认证供欧盟成员国自愿采纳，除欧盟法律或成员国法律另有规定。认证结果共有三个等级：基本（basic）、较好（substantial）和高级（High）。此外，这项网络安全法草案还会将目前的欧盟网络与信息安全局（简称 ENISA）升级为一个永久性的欧盟网络安全机构。新法规将赋予欧盟网络与信息安全局（ENISA）永久性的授权，并阐明该机构作为欧盟网络安全机构的角色。ENISA 将被赋予新任务，包括支持成员国、欧盟机构和其它利益相关者处理网络事件。ENISA 将组织常规的欧盟级网络安全演习，并支持和推动欧盟的网络安全认证政策。

4、越南国会表决通过网络安全法

新华网 6 月 12 日消息 越南第十四届国会第五次会议 6 月 12 日日以 86.86%高票通过网络安全法。该法设 7 章 43 条，对在网络空间内，就维护国家安全和社会秩序，以及各有关机构、组织和个人的行为责任做出规定。根据规定，在越南境内提供互联网相关服务的国内外企业，需将用户信息数据存储库设在越南境内，相关外国企业需在越南设立办事处。在越南境内提供互联网相关服务的国内外企业需验证用户注册信息，并应公安部门调查要求提供相关信息。该法对禁止利用网络空间煽动反对国家、歪曲历史、破坏民族团结、诽谤宗教、散布虚假和有伤风化的信息等行为做出具体规定。会议决定该法于 2019 年 1 月 1 日起正式生效。

5、埃及或将推出第一部“网络安全法”，明确 29 项处罚

E 安全 6 月 16 日消息 经过几个月的讨论，埃及议会于 2018 年 6 月 5 日通过网络犯罪法——这是埃及第一部网络相关法规，该法规以监管社交媒体内容，强化网络审查。但此法需埃及总统签署才能正式生效。这项法律旨在打击非法使用计算机和信息网络的行为，并保护埃及政府和任何公共法人的数据、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。该法还要求对宪法保障的隐私进行保护，任何人不得披露或窃听个人信息，除非取得司法命令。这项法律提出针对网络犯罪的 29 项处罚，包括 3 个月至 5 年不等的监禁，最高 2000 万埃及镑（约合人民币 718.28 万元）的罚款。

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：刘婧

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158