国家互联网应急中心

2020 年第 40 期
9 月 28 日-10 月 4 日

网络安全信息与动态周报

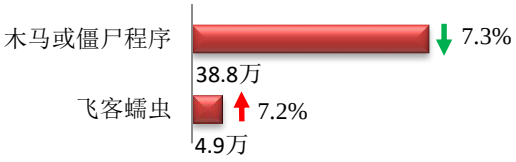
本周网络安全基本态势

境内感染网络病毒的主机数量	•43.7万	5.8%
境内被篡改网站总数 其中政府网站数量	•4556 •17	31.4% 13.3%
境内被植入后门网站总数 其中政府网站数量	•698 •1	9.9% 80.0%
针对境内网站的仿冒页面数量	•572	91.6%
新增信息安全漏洞数量 其中高危漏洞数量	•169 •44	54.2% 35.3%

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

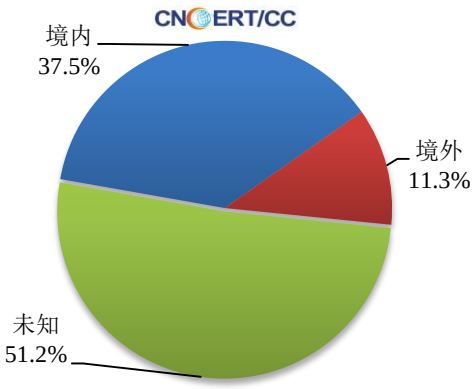
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 43.7 万个，其中包括境内被木马或被僵尸程序控制的主机约 38.8 万以及境内感染飞客（conficker）蠕虫的主机约 4.9 万。

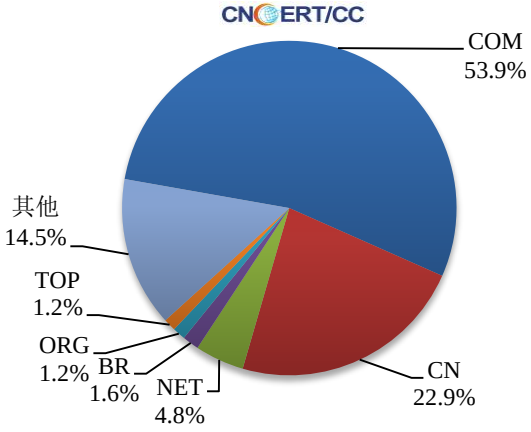


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1684 个，涉及 IP 地址 9888 个。在 1684 个域名中，有 11.3%为境外注册，且顶级域为.com 的约占 53.9%；在 9888 个 IP 中，有约 29.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 491 个 IP。

本周放马站点域名注册所属境内外分布
(9/28-10/4)



本周放马站点域名注册所属顶级域分布
(9/28-10/4)



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。

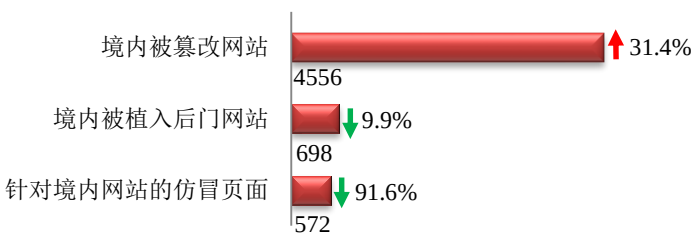
ANVA网络安全威胁信息共享平台

https://share.anva.org.cn/web/publicity/listurl

中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由 CNCERT 发起并组织运作的行业联盟。

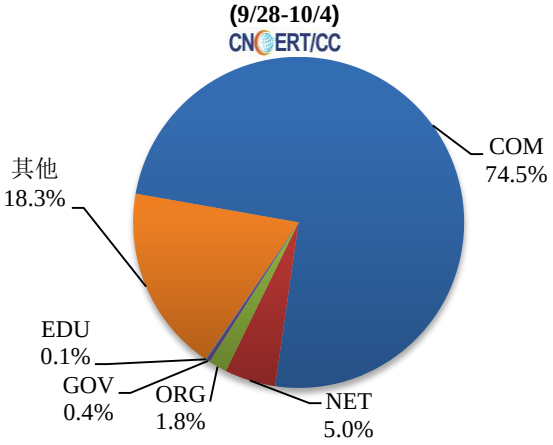
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 4556 个；被植入后门的网站数量为 698 个；针对境内网站的仿冒页面数量 572 个的仿冒页面。

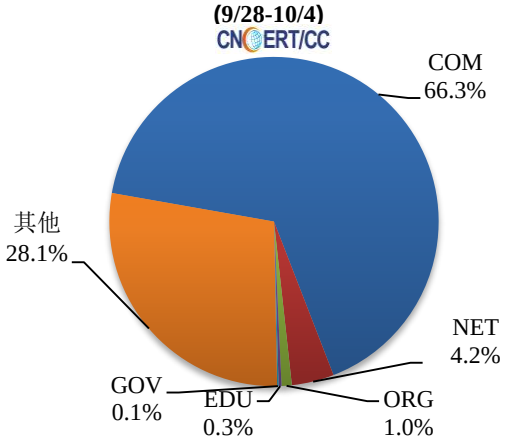


本周境内被篡改政府网站（GOV 类）数量为 17 个（约占境内 0.4%），较上周上涨了 13.3%；境内被植入后门的政府网站（GOV 类）数量为 1 个（约占境内 0.1%），较上周下降了 80.0%。

本周我国境内篡改网站按类型分布
(9/28-10/4)

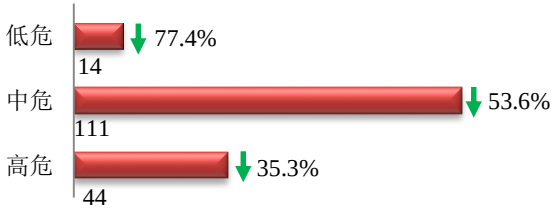


本周我国境内被植入后门网站按类型分布
(9/28-10/4)

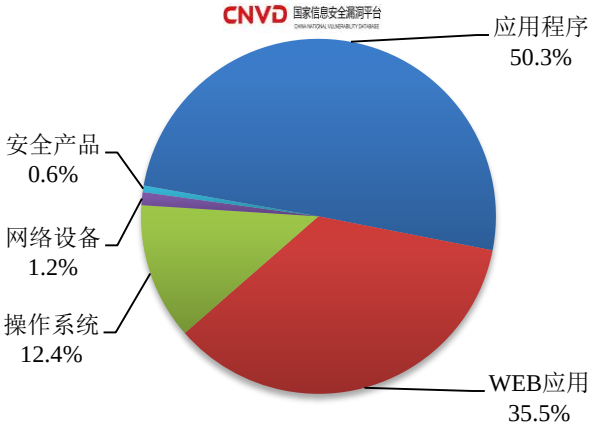


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 169 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分布
(9/28-10/4)



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 应用和操作系统。

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

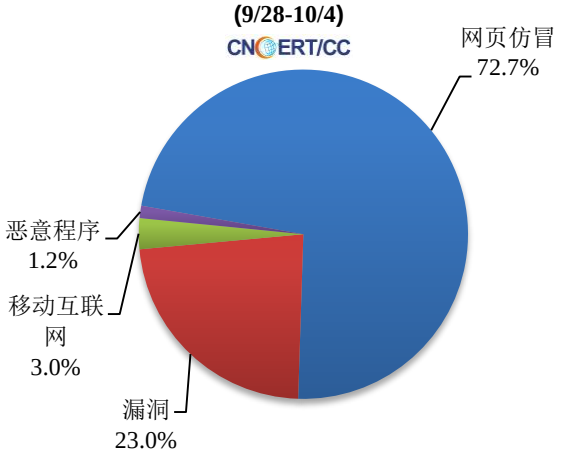
http://www.cnvd.org.cn/webinfo/list?type=4

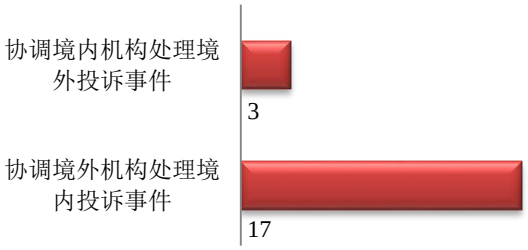
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

本周，CNCERT 协调基础电信企业、云服务商、域名注册服务机构、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 165 起，其中跨境网络安全事件 20 起。

本周CNCERT处理的事件数量按类型分布 (9/28-10/4)



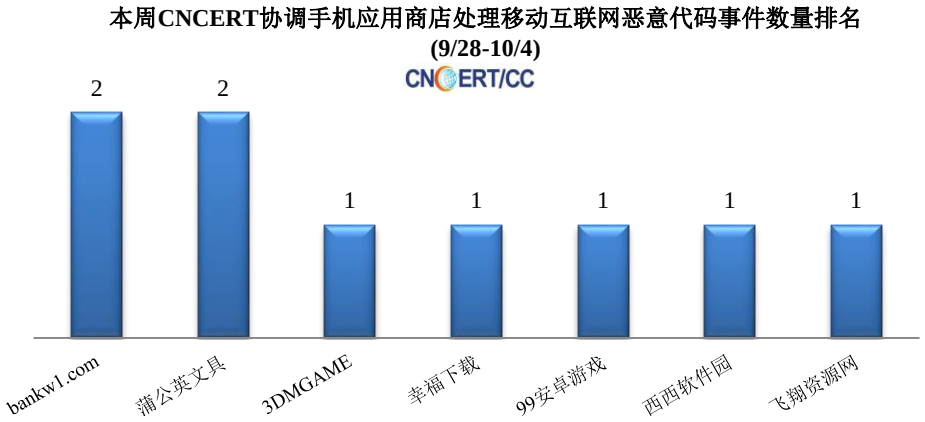


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 120 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 110 起、电子商务平台 9 起、和其他事件 1 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (9/28-10/4)

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 (9/28-10/4)

本周，CNCERT 协调 7 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 9 个。



业界新闻速递

1、 CNCERT/CC 连任 APCERT 副主席和指导委员会委员

2020 年 9 月 29 日，国家计算机网络应急技术处理协调中心（CNCERT/CC）参加了亚太地区计算机应急响应组织（APCERT）举办的 APCERT2020 年全体成员线上大会，成功竞选连任 2020-2022 年度 APCERT 指导委员会委员和 2020-2021 年度 APCERT 副主席。

本次 APCERT2020 年全体成员线上大会议程包括 APCERT 工作组会议、指导委员会委员选举、主席和副主席选举、2020 年应急演练报告、APCERT2021 年年会申办、APCERT 政策更新表决等。我中心作为 APCERT 副主席和信息共享组负责人，介绍了近一年来的工作情况及下一年的工作计划。会议进行了新一届指导委员会的选举，中国 CNCERT/CC、日本 JPCERT/CC、马来西亚 Cybersecurity Malaysia、韩国 KrCERT/CC、澳大利亚 ACSC、斯里兰卡 Sri Lanka CERT|CC、中国台北 TWNCERT 成为新一届 APCERT 指导委员会委员。随后，七个现任指导委员会委员召开内部会议选举产生 2020-2021 年度 APCERT 主席和副主席，马来西亚 Cybersecurity Malaysia 连任主席，CNCERT/CC 连任副主席。会议还宣布 APCERT2021 年年会的主办方为斯里兰卡 Sri Lanka CERT|CC,计划于 2021 年 9 月底或 10 月初举行。

APCERT 成立于 2003 年，是亚太地区计算机应急响应组织的联盟。APCERT 现有成员 32 个，来自中国、澳大利亚、日本、韩国、马来西亚等 22 个经济体，其目标是通过国际合作建立亚太地区安全、干净、可信的网络空间。

2、 医疗巨头 UHS 遭遇勒索软件攻击

9 月 29 日，据 Hackernews 报道，美国最大的医疗服务机构之一环球医疗服务公司（Universal Health Services，UHS）遭到了勒索软件的攻击。据两名知情人士透露，9 月 27 日凌晨，UHS 系统遭到攻击，全国各地包括加州和佛罗里达州的多家 UHS 机构的电脑和电话系统被锁定。其中一人说，电脑屏幕上的文字发生了变化，其中提到了“影子宇宙”，与 Ryuk 勒索软件的典型症状一致。“每个人都被告知关闭所有的电脑，不要再打开它们，”该人士说。”我们被告知，要过几天电脑才能再次启动。”目前还不知道勒索软件攻击对患者护理产生了什么影响。

3、 钓鱼邮件冒充微软更新提醒窃取用户 Outlook 凭据

9 月 28 日，据“Threstpost”网站消息，研究人员警告说，假装帮助企业员工升级到 Windows 10 的电子邮件可能会窃取他们的 Outlook 邮件和密码。这些钓鱼邮件的标题是“Re: Microsoft Windows Upgrade”，该封邮件告诉收件人，“您的 Office Windows 计算机已过时，并且计划在今天进行升级以进行替换。”邮件中还包含了一个时间表(注意，邮件中使用了奇怪的大写和空格，作为这封邮件不合法的危险信号)。然后，它告诉用户，“要升级 Windows 10，请打开浏览器到 Windows 10 升级项目网站”，指向一个 URL，该链接将收件人带到钓鱼网站登录页面。

关于国家互联网应急中心（CNCERT）

国家计算机网络应急技术处理协调中心（英文简称 CNCERT/CC），成立于 2001 年 8 月，为非政府非盈利的网络安全技术中心，是中国计算机网络应急处理体系中的牵头单位。作为国家级应急中心，CNCERT/CC 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，运行和管理国家信息安全漏洞共享平台（CNVD），维护公共互联网安全，保障关键信息基础设施的安全运行。

CNCERT/CC 在中国大陆 31 个省、自治区、直辖市设有分支机构，并通过组织网络安全企业、学校、社会组织和研究机构，协调骨干网络运营单位、域名服务机构和其他应急组织等，构建中国互联网安全应急体系，共同处理各类互联网重大网络安全事件。CNCERT/CC 积极发挥行业联动合力，发起成立了中国反网络病毒联盟（ANVA）和中国互联网网络安全威胁治理联盟（CCTGA）。

同时，CNCERT/CC 积极开展网络安全国际合作，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 2019 年，已与 78 个国家和地区的 260 个组织建立了“CNCERT/CC 国际合作伙伴”关系。CNCERT/CC 是国际应急响应与安全组织 FIRST 的正式成员，以及亚太计算机应急组织 APCERT 的发起者之一，还积极参加亚太经合组织、国际电联、上合组织、东盟、金砖等政府层面国际和区域组织的网络安全相关工作。

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：姚力

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315