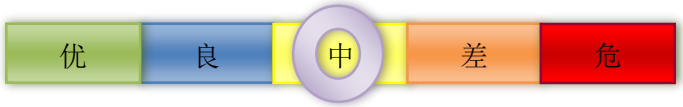
国家互联网应急中心

2020 年第 37 期
9 月 7 日-9 月 13 日

网络安全信息与动态周报

本周网络安全基本态势

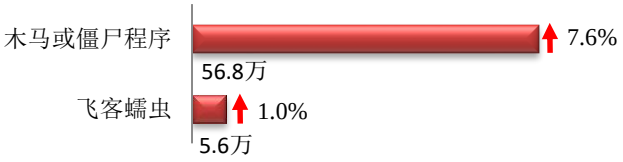


境内感染网络病毒的主机数量	•62.4万	↑ 7.0%
境内被篡改网站总数 其中政府网站数量	•3853 •18	↑ 42.3% ↑ 63.6%
境内被植入后门网站总数 其中政府网站数量	•1277 •36	↑ 10.3% ↑ 800.0%
针对境内网站的仿冒页面数量	•15029	↓ 14.3%
新增信息安全漏洞数量 其中高危漏洞数量	•395 •142	↓ 15.1% ↑ 8.4%

= 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

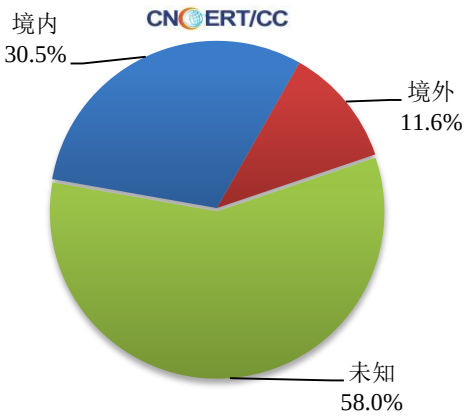
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 62.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 56.8 万以及境内感染飞客（conficker）蠕虫的主机约 5.6 万。

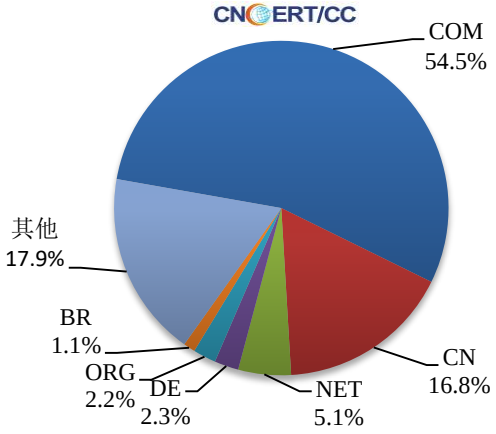


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1668 个，涉及 IP 地址 6380 个。在 1668 个域名中，有 11.6%为境外注册，且顶级域为.com 的约占 54.5%；在 6380 个 IP 中，有约 64.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 292 个 IP。

本周放马站点域名注册所属境内外分布
(9/7-9/13)



本周放马站点域名注册所属顶级域分布
(9/7-9/13)



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。

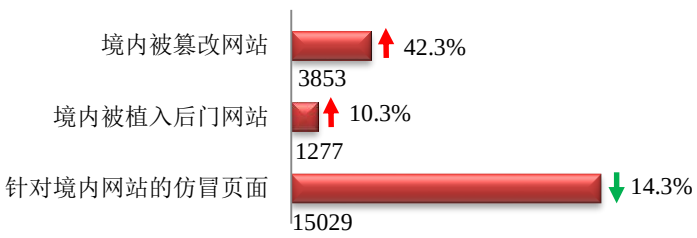
ANVA网络安全威胁信息共享平台

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。

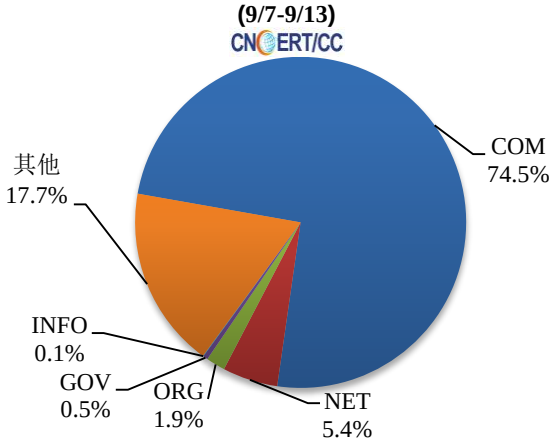
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 3853 个；被植入后门的网站数量为 1277 个；针对境内网站的仿冒页面数量 15029 个的仿冒页面。

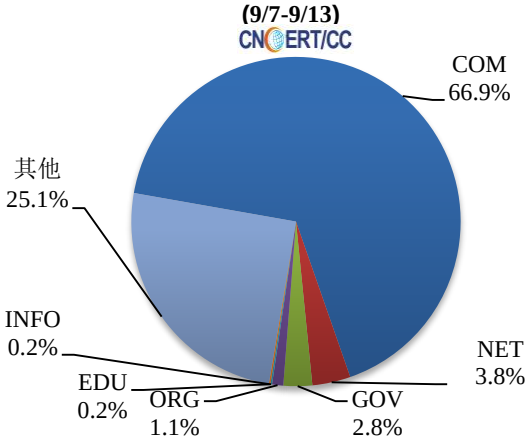


本周境内被篡改政府网站（GOV 类）数量为 18 个（约占境内 0.5%），较上周上涨了 63.6%；境内被植入后门的政府网站（GOV 类）数量为 36 个（约占境内 2.8%），较上周上涨了 800.0%。

本周我国境内篡改网站按类型分布
(9/7-9/13)

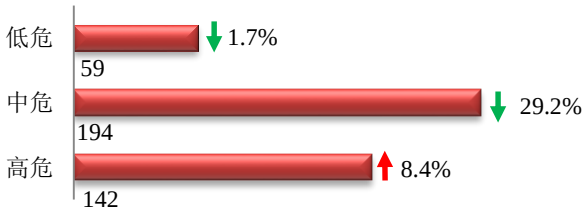


本周我国境内被植入后门网站按类型分布
(9/7-9/13)

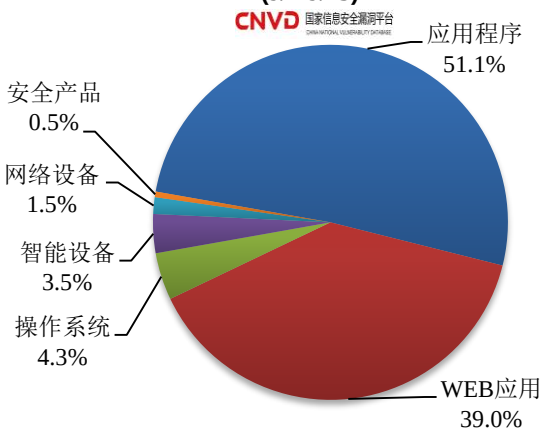


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 395 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
(9/7-9/13)



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

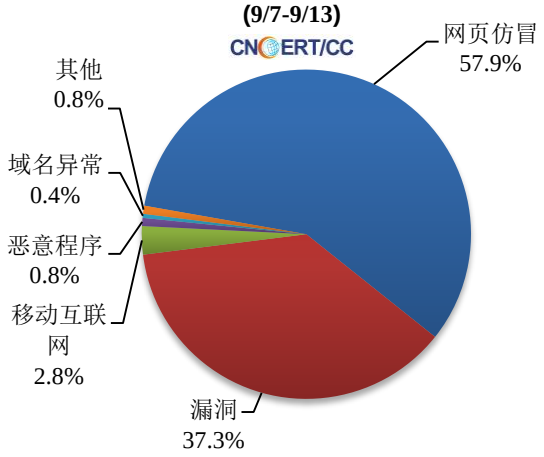
http://www.cnvd.org.cn/webinfo/list?type=4

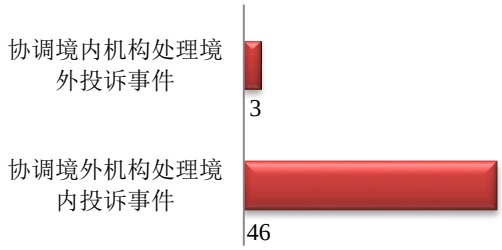
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 252 起，其中跨境网络安全事件 49 起。

本周CNCERT处理的事件数量按类型分布 (9/7-9/13)

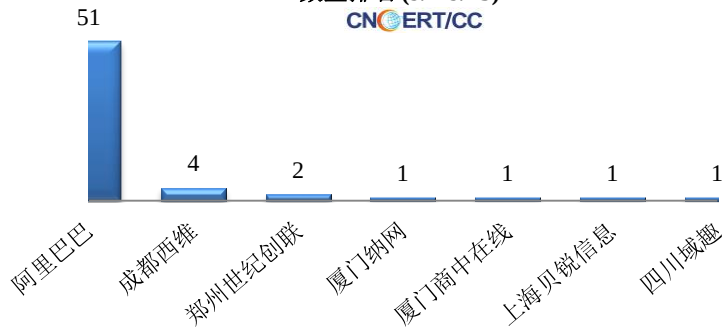




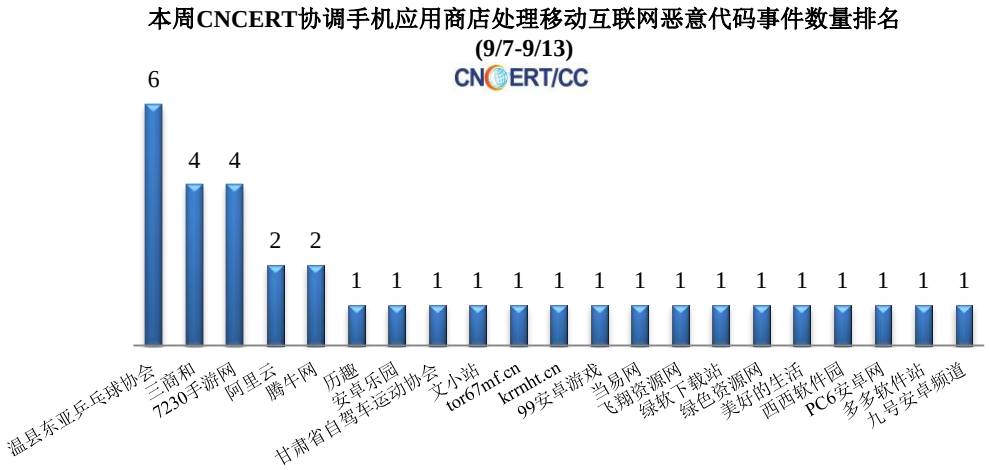
本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 146 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 134 起、电子商务平台 10 起和其他事件 2 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (9/7-9/13)

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 (9/7-9/13)



本周，CNCERT 协调 21 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 34 个。



业界新闻速递

1、 2020 年国家网络安全宣传周将于 9 月 14 日至 20 日举行

9 月 5 日，据中国网信网消息，9 月 4 日，2020 年国家网络安全宣传周新闻发布会在京举行。中央网信办网络安全协调局副局长、一级巡视员高林，郑州市委常委、宣传部部长黄卿介绍 2020 年国家网络安全宣传周活动筹备情况，并答记者问。2020 年国家网络安全宣传周将于 9 月 14 日至 20 日在全国范围内统一开展，主题为“网络安全为人民，网络安全靠人民”，由中央宣传部、中央网信办、教育部、工业和信息化部、公安部、中国人民银行、国家广播电视总局、全国总工会、共青团中央、全国妇联等部门联合举办。会上透露，今年网安周的网络安全高峰论坛等重要活动将在河南省郑州市举行，主要内容包括：网络安全高峰论坛、数字化展会、网安周特别节目、全民网络安全知识竞赛、线上网络安全课堂、主题日等活动等相继举办。

2、 Visa 发现一款新型信用卡窃取器 能够规避检测并窃取用户卡内数据

9 月 8 日，据外媒报道，Visa 发布了一项关于新的信用卡 JavaScript 窃取器的警告，它被称为 Baka，这种电子窃取器会在窃取银行卡信息后自动从内存中删除，实现了规避检测的新功能。专家在全球多个使用 Visa eTD 功能的商家网站上发现了 Baka 窃取器。Baka 窃取器的工作原理是动态地向远程 JavaScript 文件加载当前页面，添加脚本标记。JavaScript 网址以加密格式硬编码在加载器脚本中，攻击者可以更改每个受害者的网址。据了解，Baka 是第一个使用 XOR 密码对硬编码进行加密的 JavaScript 窃取恶意软件。

3、 智利银行在勒索软件攻击后关闭所有分行

9 月 8 日，科技行者网站消息，智利三大银行之一的国家银行（BancoEstado）上周末遭到勒索软件攻击，7 日宣布关闭所有分支机构。有关攻击的细节尚未公开，但消息来源称该银行计算机感染的是 REvil (Sodinokibi)勒索软件。攻击始于一位雇员收到并打开了一份恶意 Office 文档，文档执行在银行的网络安装了一个后门。在 4 日至 5 日晚上，黑客利用后门访问了银行的内网安装了勒索软件。一开始，银行试图在不被注意的情况下恢复服务，但破坏范围太广，勒索软件加密了该行的大部分内部服务和雇员工作站。银行在 6 日披露了攻击，官员认识到他们也难以快速恢复服务，因此决定关闭分行。银行的网站、入口、移动应用，以及 ATM 机器都未受到影响。

4、 Mykings 僵尸网络新变种通过 PcShare 远程控制，已感染超 5 万台电脑挖矿

9 月 11 日，腾讯安全威胁情报中心检测到 Mykings 挖矿僵尸网络变种木马，更新后的 Mykings 会在被感染系统安装开源远程控制木马 PcShare，对受害电脑进行远程控制，可进行操作文件、服务、注册表、进程、窗口等多种资源，并且可以下载和执行指定的程序。Mykings 僵尸网络木马还会关闭 Windows Defender、检测卸载常见杀毒软件；卸载竞品挖矿木马和旧版挖矿木马；下载“暗云”木马感染硬盘主引导记录（MBR)实现长期驻留；通过计划任务、添加启动项等实现开机自动运行等行为。由于 MyKings 僵尸网络主动扩散的能力较强，影响范围较广，对企业用户危害严重。根据推测，Mykings 僵尸网络目前已控制超过 5 万台电脑进行挖矿作业。

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 2019 年，CNCERT 已与 78 个国家和地区的 260 个组织建立了“CNCERT 国际合作伙伴”关系。CNCERT 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：狄少嘉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315