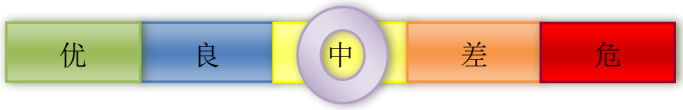
国家互联网应急中心

2020 年第 45 期
11 月 2 日-11 月 8 日

# 网络安全信息与动态周报

## 本周网络安全基本态势

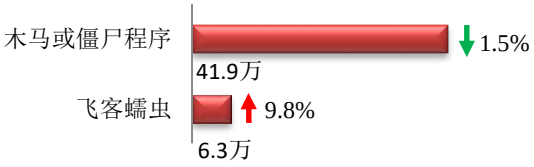



| | | |
|---|---|---|
| 境内感染网络病毒的主机数量 | •48.2万 | 0.1% |
| 境内被篡改网站总数<br>其中政府网站数量 | •97<br>•2 | 97.9%<br>92.3% |
| 境内被植入后门网站总数<br>其中政府网站数量 | •819<br>•21 | 40.5%<br>950.0% |
| 针对境内网站的仿冒页面数量 | •2655 | 347.0% |
| 新增信息安全漏洞数量<br>其中高危漏洞数量 | •340<br>•113 | 18.7%<br>17.5% |

*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*

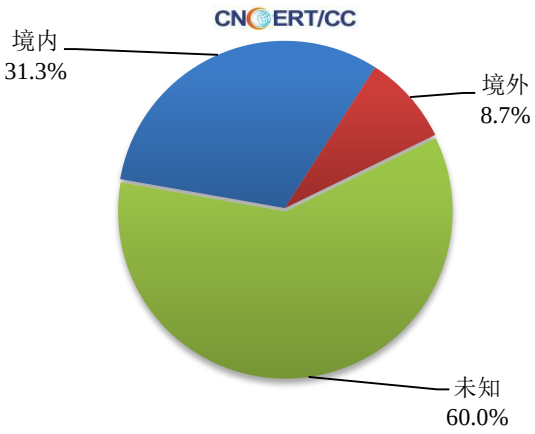
## 本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 48.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 41.9 万以及境内感染飞客（conficker）蠕虫的主机约 6.3 万。

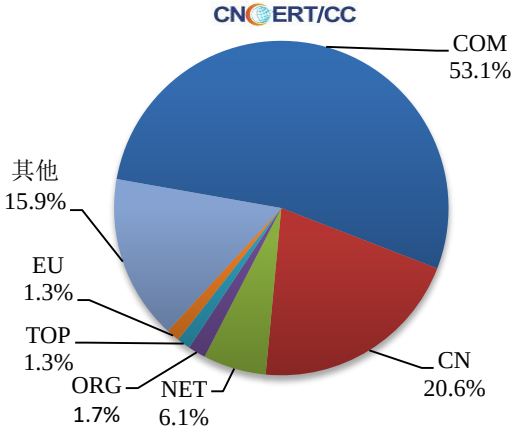


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1872 个，涉及 IP 地址 7458 个。在 1872 个域名中，有 8.7%为境外注册，且顶级域为.com 的约占 53.1%；在 7458 个 IP 中，有约 22.9%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 628 个 IP。

**本周放马站点域名注册所属境内外分布**
**(11/02-11/08)**




**本周放马站点域名注册所属顶级域分布**
**(11/02-11/08)**




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。

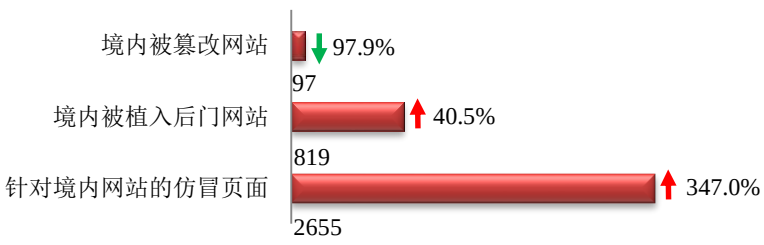
**ANVA网络安全威胁信息共享平台**

**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。*

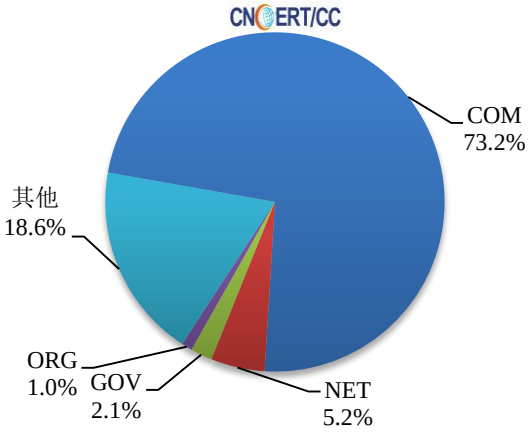
## 本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 97 个；被植入后门的网站数量为 819 个；针对境内网站的仿冒页面数量 2655 个的仿冒页面。

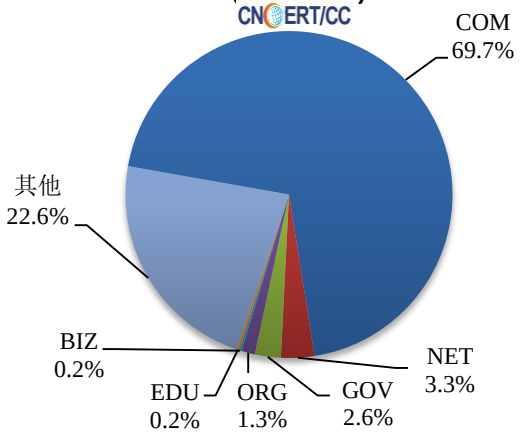


本周境内被篡改政府网站（GOV 类）数量为 2 个（约占境内 2.1%），较上周下降了 92.3%；境内被植入后门的政府网站（GOV 类）数量为 21 个（约占境内 2.6%），较上周上涨了 950.0%。

**本周我国境内篡改网站按类型分布**
**(11/02-11/08)**

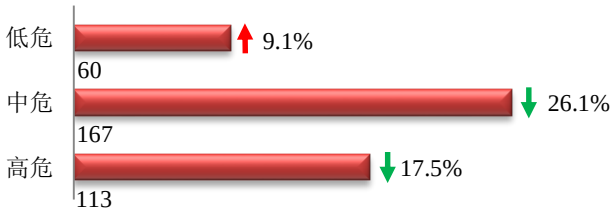



**本周我国境内被植入后门网站按类型分布**
**(11/02-11/08)**

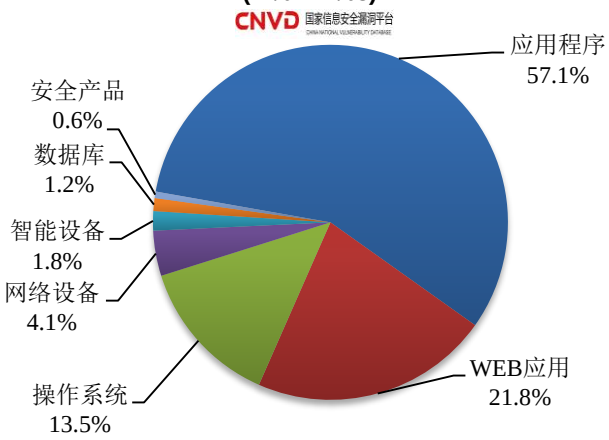



## 本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 340 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**
**(11/02-11/08)**




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**

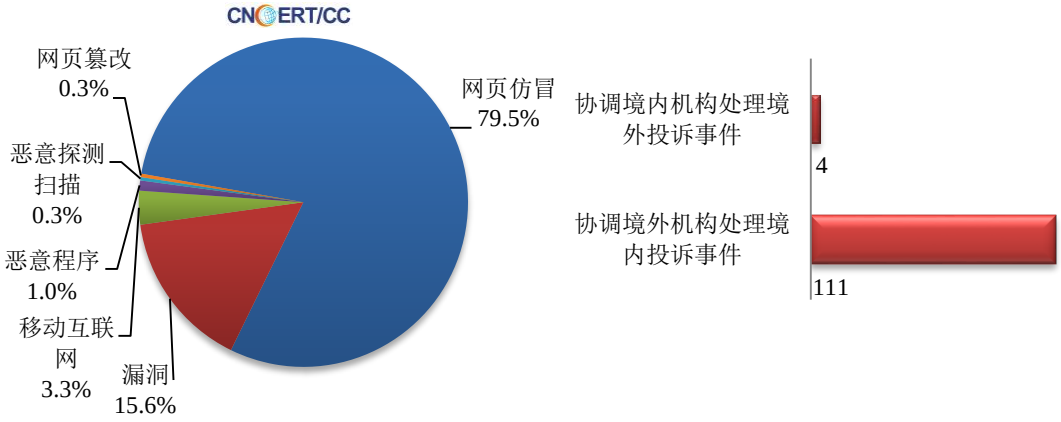
http://www.cnvd.org.cn/webinfo/list?type=4

*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 302 起，其中跨境网络安全事件 115 起。

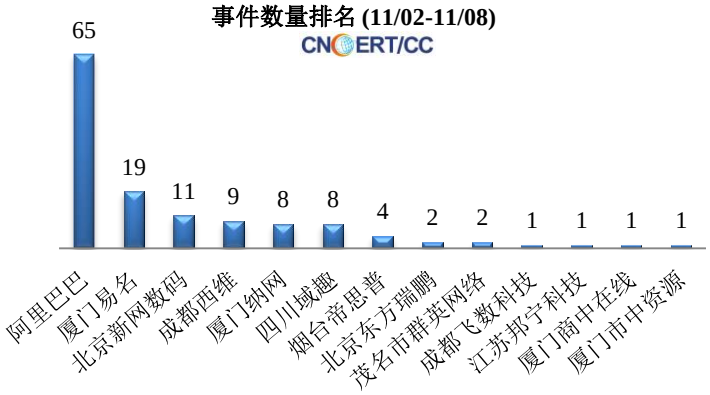
**本周CNCERT处理的事件数量按类型分布**
**(11/02-11/08)**



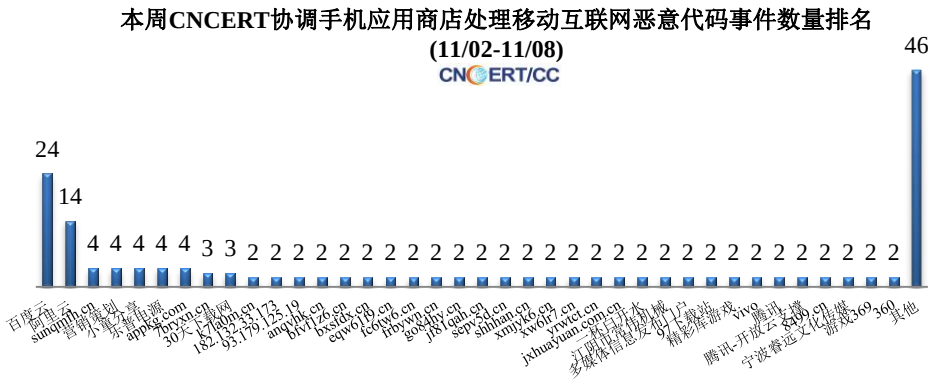

本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 240 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 178 起、电子商务平台 60 起以及其他事件 2 起。

**本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计**
**(11/02-11/08)**


**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 (11/02-11/08)**



本周，CNCERT 协调 84 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 168 个。




## 业界新闻速递

### 1. 世界互联网大会•互联网发展论坛将于 11 月 23 日至 24 日举行

11 月 2 日，中国网信网消息，11 月 2 日下午，世界互联网大会•互联网发展论坛新闻发布会在京举行，宣布互联网发展论坛将于 11 月 23 日至 24 日在浙江乌镇举行。本次论坛由世界互联网大会组委会主办，主题为“数字赋能 共创未来——携手构建网络空间命运共同体”。国家网信办副主任赵泽良，浙江省委常委、省委宣传部部长朱国贤等出席发布会并回答记者提问。

赵泽良表示，今年以来，新冠肺炎疫情在全球蔓延，国际形势深刻变革，在这样的背景下，秉持网络空间命运共同体理念，努力推动全球网络空间向更加包容、平衡、共赢方向发展，显得尤为重要。基于这样的考虑，世界互联网大会积极探索办会新模式、新路径，多维、立体展示推动互联网发展治理的中国方案、中国智慧和中国担当。与往年相比，今年论坛有三方面新变化：一是办会形式有新创意，取消举办第七届世界互联网大会，改为举办“世界互联网大会•互联网发展论坛”；二是论坛规模有新调整，论坛呈现“小而精”“新而活”的崭新面貌；三是参会方式有新设计，以“线下+线上”形式开展各项活动。论坛也有很多“不变”的地方，整体上保持了世界互联网大会一贯的风格和精神内核。

朱国贤介绍，浙江将充分发挥用互联网引领时代潮流、造福人类进步、创造美好生活、赋能未来发展的窗口作用。秉持智能办会，确保论坛安全出彩，实现智能办会与安全办会相统一；坚持守正创新，力求论坛呈现简约精彩，新建“一馆一园一场”，推动互联网元素更深入地融入乌镇的文化基因；聚焦数字赋能，推动论坛成果绽放异彩，为全省发展注入“澎湃动力”。

据悉，今年的论坛设置 1 场主论坛和 5 场分论坛。期间将继续举办丰富多彩的配套活动，世界互联网领先科技成果发布活动将发布 15 项左右年度前沿互联网科技成果。“互联网之光”博览会将瞄准

世界互联网最新发展趋势和前沿技术动态，展示具有全球引领力和创新力的技术成果、产品应用。“直通乌镇”全球互联网大赛主要展现数字抗疫和互联网创新成果，释放创新创业活力。此外，本次论坛还将发布《世界互联网发展报告 2020》和《中国互联网发展报告 2020》蓝皮书等成果性文件。

## 2. Google Play 商店应用强制删除了 17 款感染恶意软件的应用程序

11 月 2 日，cnBeta 网站消息，谷歌官方 Play Store 删除了 17 款 Android 应用程序。据来自 Zscaler 的安全研究人员 Viral Gandhi 称，这 17 个应用程序全部感染了 Joker（又名 Bread）恶意软件。该软件旨在窃取短信、联系人名单和设备信息。据调查发现，这批病毒软件从 3 月份开始活跃，已经成功感染了数百万台设备。虽然谷歌从 Play Store 中删除了这些应用程序，但已感染设备用户仍需手动从设备中删除。

## 3. 勒索软件组织 Maze 宣布“正式关闭”

11 月 3 日，cnBeta 网站消息，在 11 月 1 日，最活跃、最臭名昭著的数据窃取勒索软件组织之一 Maze 宣布“正式关闭”。该公告令人费解，公告中不仅多处出现拼写错误，而且是在暗网网站上发布的。在过去一年中，该组织已针对大量目标公司发起了攻击，包括信息技术咨询及业务流程提供商 Cognizant、网络安全保险公司 Chubb、制药巨头 ExecuPharm、特斯拉和 SpaceX 的零件供应商 Visser 和国防承包商 Kimchuk。Maze 最初使用漏洞攻击工具包和垃圾邮件活动来感染受害者，但后来开始使用已知的安全漏洞专门针对大型公司。Maze 随后使用易受攻击的虚拟专用网（VPN）和远程桌面（RDP）服务器对受害者的网络发动有针对性的攻击。

## 4. Adobe 已经修复了 Acrobat 产品中的 14 个漏洞

11 月 3 日，SECURITYWEEK 网站消息，Adobe 表示，已经在 Windows 和 macOS 版本的 Acrobat DC、Acrobat Reader DC、Acrobat 2020、Acrobat Reader 2020、Acrobat 2017 和 Acrobat Reader 2017 中修复了 14 个安全漏洞。其中三个漏洞被评为严重级别，它们是由释放后使用、基于堆的缓冲区溢出和越界写入错误引起的。

## 5. 巴西高等司法法院遭遇重大网络攻击事件

11 月 6 日，据外媒 ZDNet 报道，巴西高等司法法院(STJ) 3 日遭遇重大网络攻击，将使其业务停顿整整一周。攻击发生时有几个审判正在进行。据 STJ 称，在法院的网络中发现了一种病毒，作为预防措施，与互联网的链接被切断，促使审判会议被取消。法院的所有系统，包括电子邮件以及电话系统也因此无法使用。STJ 部长 Humberto Martins 5 日就这一事件发表声明，称此次攻击并没有影响到

正在进行的法院诉讼的相关信息。根据部长的描述，虽然入侵利用加密技术阻止了数据访问，但有备份。可后来攻击也影响了法院的备份，这次攻击事件被称为巴西有史以来最严重的网络安全事件。

## 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：吕利锋

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315