国家互联网应急中心

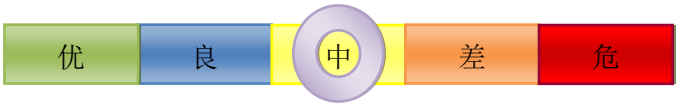
# 网络安全信息与动态周报

**2020 年第 47 期**

**11 月 16 日-11 月 22 日**

CNCERT/CC

## 本周网络安全基本态势

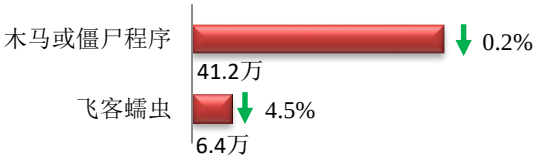



| | | |
|---|---|---|
| 境内感染网络病毒的主机数量 | •47.6万 | 0.8% |
| 境内被篡改网站总数<br>其中政府网站数量 | •4241<br>•18 | 7.1%<br>18.2% |
| 境内被植入后门网站总数<br>其中政府网站数量 | •902<br>•31 | 19.5%<br>158.3% |
| 针对境内网站的仿冒页面数量 | •6970 | 95.0% |
| 新增信息安全漏洞数量<br>其中高危漏洞数量 | •477<br>•109 | 33.4%<br>55.9% |

*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*

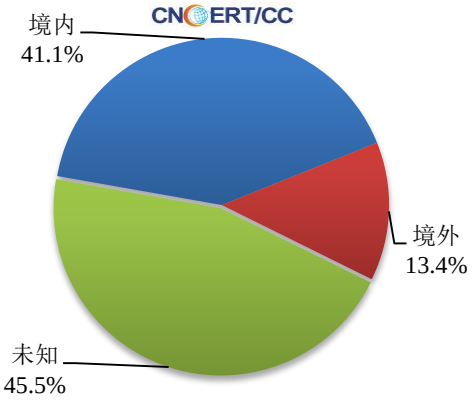
## 本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 47.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 41.2 万以及境内感染飞客（conficker）蠕虫的主机约 6.4 万。

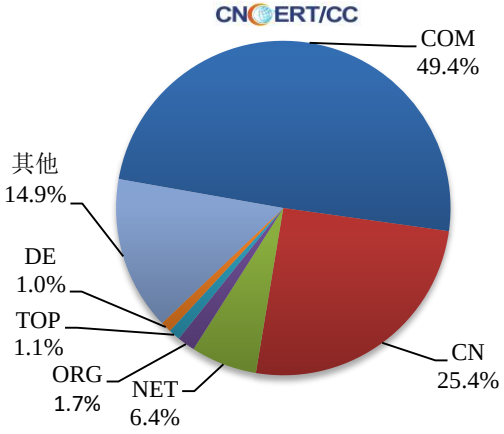


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1157 个，涉及 IP 地址 6121 个。在 1157 个域名中，有 13.4%为境外注册，且顶级域为.com 的约占 49.4%；在 6121 个 IP 中，有约 26.9%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 566 个 IP。

**本周放马站点域名注册所属境内外分布**
**(11/16-11/22)**




**本周放马站点域名注册所属顶级域分布**
**(11/16-11/22)**




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。

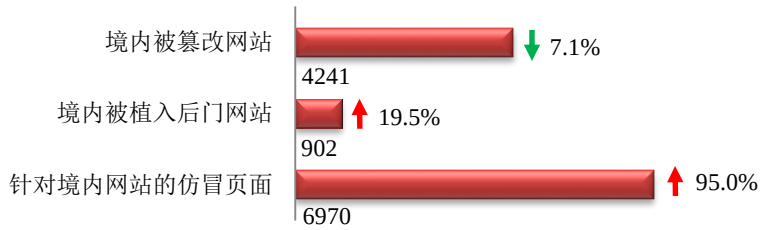
**ANVA网络安全威胁信息共享平台**

**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。*

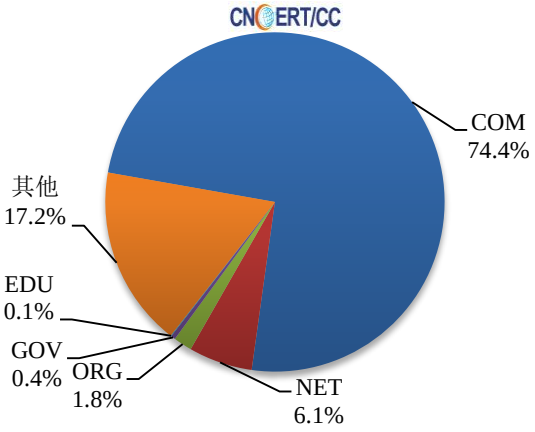
## 本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 4241 个，主要是完善了监测规则；被植入后门的网站数量为 902 个；针对境内网站的仿冒页面数量 6970 个的仿冒页面。

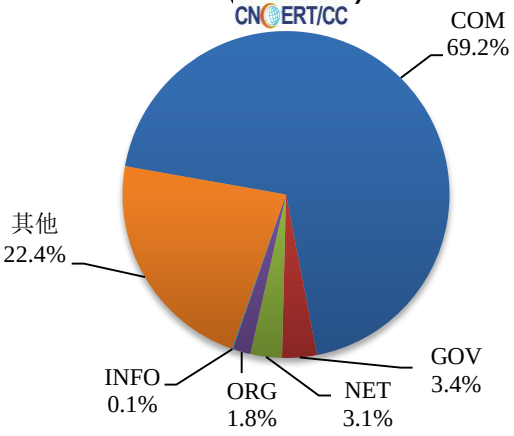


本周境内被篡改政府网站（GOV 类）数量为 18 个（约占境内 0.4%），较上周下降了 18.2%；境内被植入后门的政府网站（GOV 类）数量为 31 个（约占境内 3.4%），较上周上涨了 158.3%。

**本周我国境内篡改网站按类型分布**
**(11/16-11/22)**

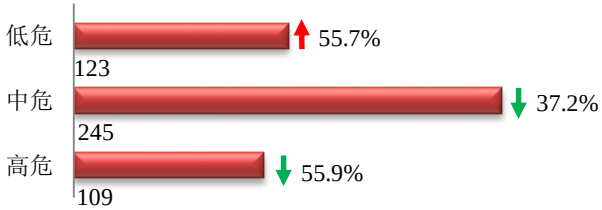



**本周我国境内被植入后门网站按类型分布**
**(11/16-11/22)**

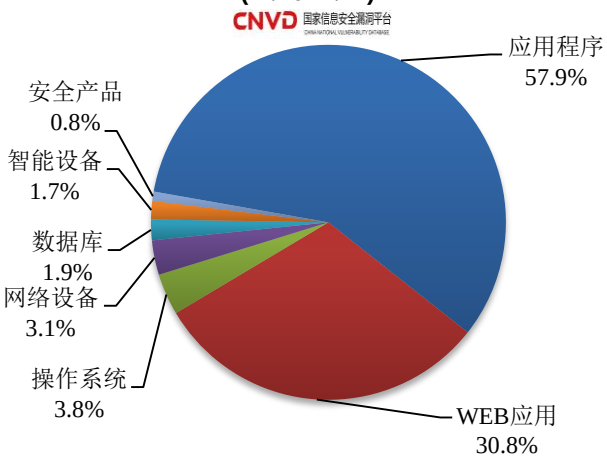



## 本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 477 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**
**(11/16-11/22)**




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**

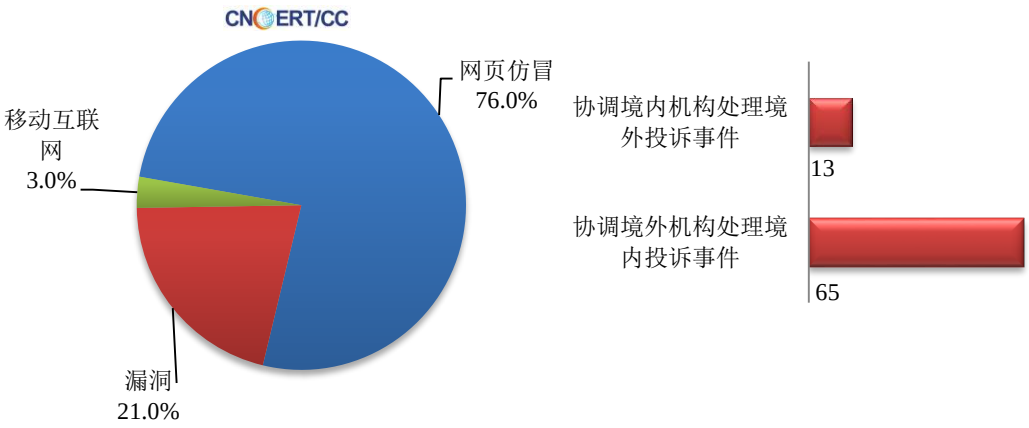
http://www.cnvd.org.cn/webinfo/list?type=4

*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

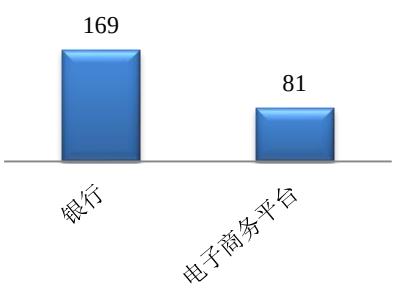
本周，CNCERT 协调基础电信企业、云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 329 起，其中跨境网络安全事件 78 起。

**本周CNCERT处理的事件数量按类型分布**
**(11/16-11/22)**

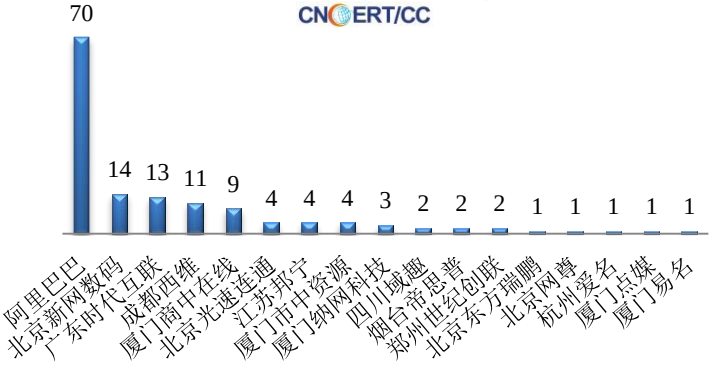



本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 250 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 169 起、电子商务平台 81 起。

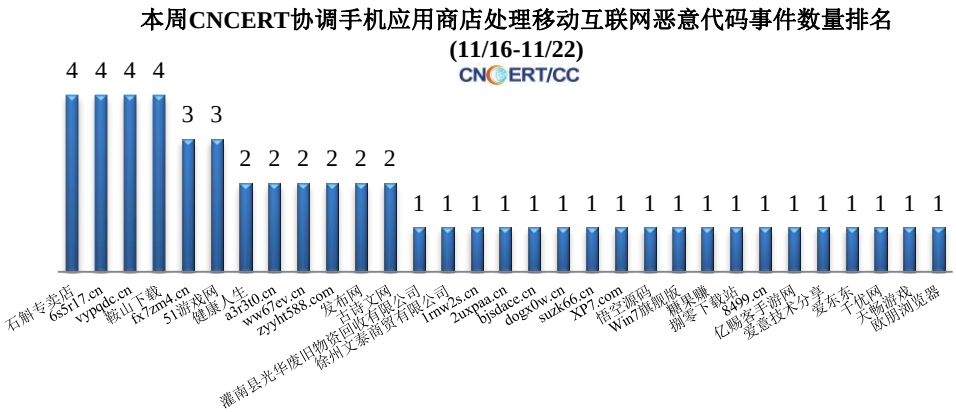
**本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计**
**(11/16-11/22)**




**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 (11/16-11/22)**



本周，CNCERT 协调 31 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 53 个。




## 业界新闻速递

### 1. 关于 35 款 App 存在个人信息收集使用问题的通告

11 月 17 日，中国网信网消息，近期 App 违法违规收集使用个人信息治理工作组评估发现，35 款 App 存在个人信息收集使用问题，建议相关 App 运营者及时对存在的问题进行整改，并自即日起 30 日内向工作组反馈整改情况。30 日后工作组将对整改情况进行核验，并向相关部门提交复核结果，对不能有效整改的建议依法予以处置。

### 2. 世界互联网大会组委会发布《携手构建网络空间命运共同体行动倡议》

11 月 18 日，新华社北京电（记者 余俊杰）世界互联网大会组委会发布的《携手构建网络空间命运共同体行动倡议》指出，国际社会应采取更加积极、包容、协调、普惠的政策，加快全球信息基础设施建设，促进互联互通，推动数字经济创新发展。

这份 18 日发布的倡议强调，在当前疫情背景下，构建网络空间命运共同体的重要性和紧迫性更加凸显。面对新的风险和挑战，国际社会在网络空间领域应加强团结协作、维护公平正义、共享数字红利。

倡议呼吁，各国政府、国际组织、互联网企业、技术社群、社会组织和公民个人坚持共商共建共享的全球治理观，秉持“发展共同推进、安全共同维护、治理共同参与、成果共同分享”的理念，把网络空间建设成为造福全人类的发展共同体、安全共同体、责任共同体、利益共同体。

在网络安全领域，倡议呼吁开展全球、区域、多边等各层级的合作与对话，共同维护网络空间和平与稳定，增进各国之间战略互信，反对网络攻击、网络威慑与讹诈，反对利用信息技术破坏他国关键信息基础设施或窃取重要数据。

倡议呼吁加强对弱势群体的支持和帮助，坚持以人为本、科技向善，采取多种政策措施和技术手段，提高弱势群体的数字技能，促进公众数字素养的提升。

此外，倡议还呼吁畅通贸易渠道，探索建立信息共享和互信互认机制，减少市场准入壁垒和其他壁垒，鼓励使用安全可靠的数字化手段促进跨境贸易便利化，共享电子商务发展红利。

### 3. 游戏公司 Capcom 数据遭攻击泄露

11 月 16 日，据“bleepingcomputer”网站消息，11 月 2 日，日本游戏巨头 Capcom 遭到网络攻击，攻击者窃取了客户和员工的信息，导致他们关闭部分网络以阻止感染的传播。安全研究人员对攻击的恶意软件样本进行分析后确定是 Ragnar Locker 勒索软件发起的网络攻击。尽管几乎所有的勒索软件操作都是在加密设备之前窃取未加密文件，作为双重勒索策略，但在 11 月 4 日的新闻发布会上 Capcom 公司表示，没有迹象表明任何数据被盗。然而，他们的声明与 Ragnar Locker 在其网站上发布的被盗数据样本和赎金记录矛盾。16 日，Capcom 发布了数据泄露公告，承认了此次攻击不仅导致公司机密文件被盗，客户和员工数据也被窃取。在攻击过程中，黑客可以访问客户的姓名，地址，性别，电话号码，电子邮件地址，出生日期，投资者姓名，持股量和照片。员工暴露的信息可能包括姓名，地址，护照信息，签名，生日，电话号码，照片，电子邮件地址等。

### 4. 加密货币交易所 Liquid 遭受黑客攻击

11 月 18 日，据 ZDnet 报道，当今排名前 20 位的加密货币交换门户之一的 Liquid 在 11 月 13 日被黑客突破了 Liquid 员工的电子邮件帐户，并转移到公司内部网络。该公司表示，在黑客窃取资金之前就已检测到入侵，但随后的调查显示，攻击者能够从 Liquid 存储用户信息的数据库中收集个人信息。被盗信息包括真实姓名、家庭住址、电子邮件和加密密码。Liquid 首席执行官表示，公司仍在调查入侵者是否能够窃取所有用户在平台上进行首次交易时必须提供的身份证明。

### 5. 网站托管服务提供商 Managed 遭勒索软件攻击

11 月 19 日，据“Security Affairs”网站消息，网站托管服务提供商 Managed 在上周末受到 REvil 勒索软件攻击，导致他们的服务器和托管系统脱机。Managed 最初表示，该事件只影响了少数客户网站，但几个小时后，它被迫关闭了整个网站托管基础设施。受影响的系统包括 WordPress 和 DotNetNuke 管理主机平台、在线数据库、电子邮件服务器、DNS 服务器、RDP 访问点和 FTP 服务器。Managed 向执法部门报告了这一事件，并开始着手恢复其基础设施。

## 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：何能强

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315