国家互联网应急中心

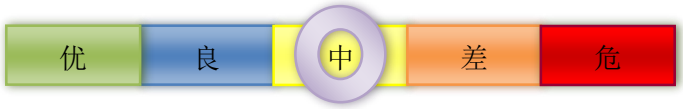
2020 年第 46 期

11 月 9 日-11 月 15 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

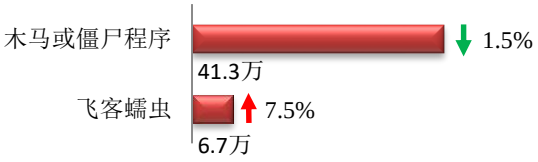


境内感染网络病毒的主机数量	•48.0万	0.3%
境内被篡改网站总数 其中政府网站数量	•4565 •22	4606.2% 1000.0%
境内被植入后门网站总数 其中政府网站数量	•755 •12	7.8% 42.9%
针对境内网站的仿冒页面数量	•3575	34.7%
新增信息安全漏洞数量 其中高危漏洞数量	•716 •247	110.6% 118.6%

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*

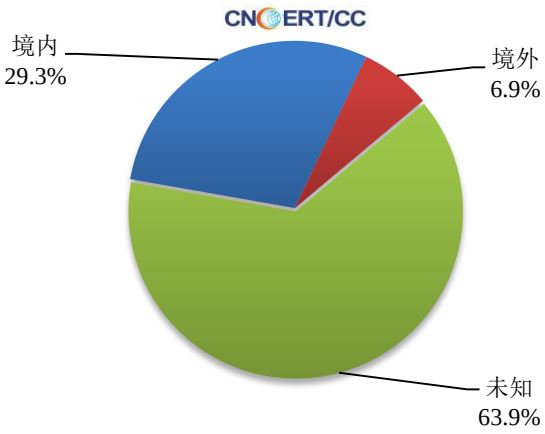
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 48.0 万个，其中包括境内被木马或被僵尸程序控制的主机约 41.3 万以及境内感染飞客（conficker）蠕虫的主机约 6.7 万。

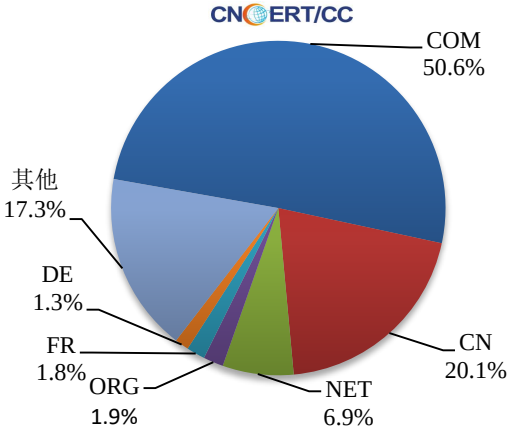


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1340 个，涉及 IP 地址 5251 个。在 1340 个域名中，有 6.9%为境外注册，且顶级域为.com 的约占 50.6%；在 5251 个 IP 中，有约 23.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 507 个 IP。

本周放马站点域名注册所属境内外分布
(11/09-11/15)



本周放马站点域名注册所属顶级域分布
(11/09-11/15)



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。

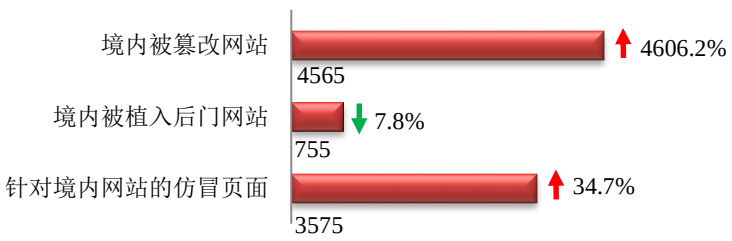
ANVA网络安全威胁信息共享平台

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。

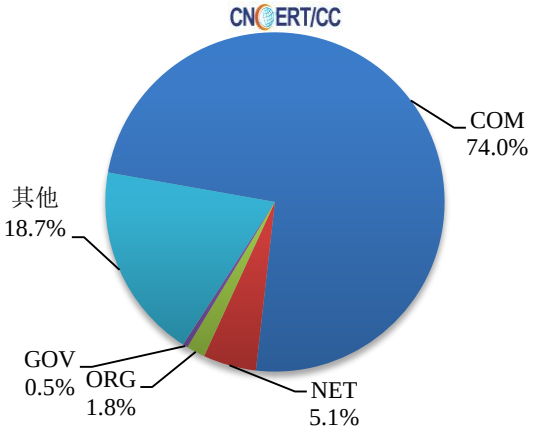
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 4565 个，主要是完善了监测规则；被植入后门的网站数量为 755 个；针对境内网站的仿冒页面数量 3575 个的仿冒页面。

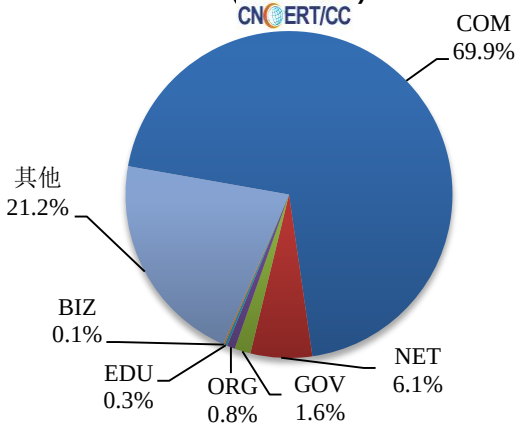


本周境内被篡改政府网站（GOV 类）数量为 22 个（约占境内 0.5%），较上周上涨了 1000.0%；境内被植入后门的政府网站（GOV 类）数量为 12 个（约占境内 1.6%），较上周下降了 42.9%。

本周我国境内篡改网站按类型分布
(11/09-11/15)

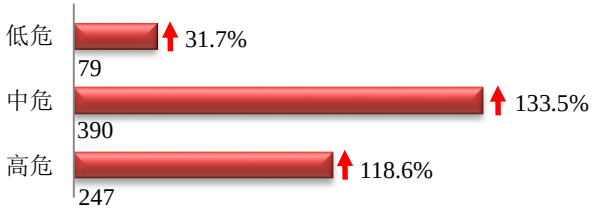


本周我国境内被植入后门网站按类型分布
(11/09-11/15)

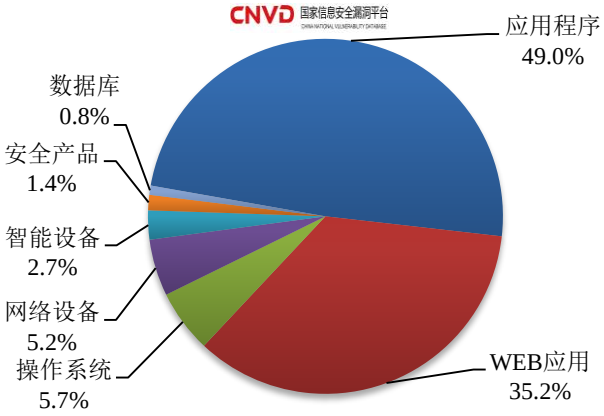


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 716 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
(11/09-11/15)



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

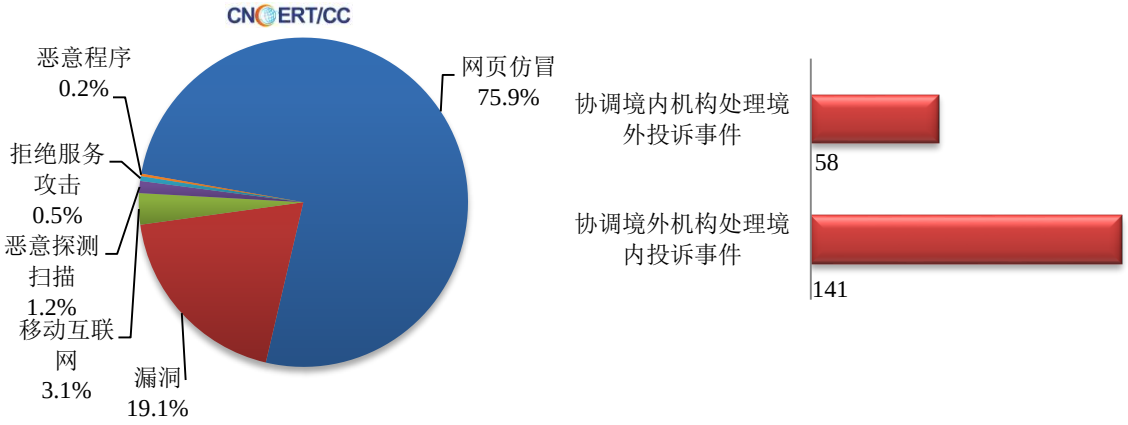
http://www.cnvd.org.cn/webinfo/list?type=4

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

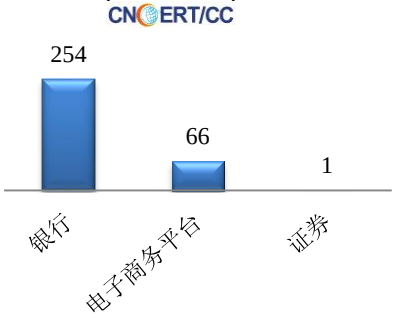
本周，CNCERT 协调基础电信企业、云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 423 起，其中跨境网络安全事件 199 起。

本周CNCERT处理的事件数量按类型分布
(11/09-11/15)

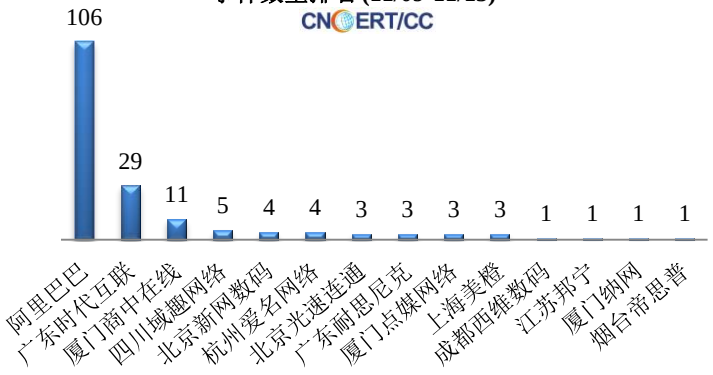


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 321 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 254 起、电子商务平台 66 起以及证券事件 1 起。

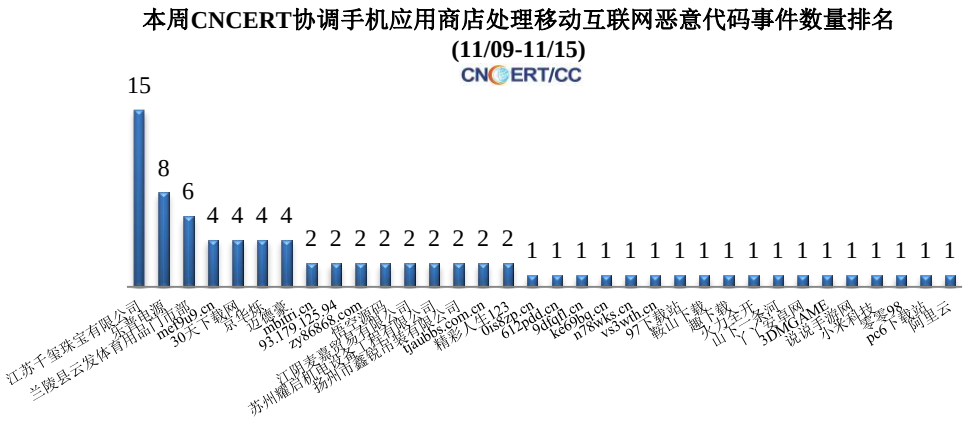
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计
(11/09-11/15)



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 (11/09-11/15)



本周，CNCERT 协调 34 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 81 个。



业界新闻速递

1. 工业和信息化部通报下架 60 款侵害用户权益 APP

11 月 10 日，工业和信息化部官网消息，2020 年 10 月 26 日，向社会通报了 131 家存在侵害用户权益行为 APP 企业的名单。截至目前，经第三方检测机构核查复检，尚有 60 款 APP 未按照工业和信息化部要求完成整改。依据《网络安全法》和《移动智能终端应用软件预置和分发管理暂行规定》（工信部信管〔2016〕407 号）等法律和规范性文件要求，工业和信息化部组织对该 60 款 APP 进行下架。

相关应用商店应在本通报发布后，立即组织对名单中应用软件进行下架处理。后续，工业和信息化部还将对未严格落实管理主体责任的部分应用商店及移动应用分发平台，存在违规收集用户个人信息行为的 SDK 企业，依法严厉处置。

2. 研究人员发现 Linux 版本的勒索软件

11 月 6 日，安全公司卡巴斯基发布报告称，其发现一款针对 Linux 平台的 RansomEXX 勒索软件，标志着肆虐 Windows 平台的勒索软件变种首次波及 Linux 平台。RansomEXX 勒索软件主要针对难以承受停机风险的企业和政府机构，黑客通过将恶意软件散播到更多的网络和系统，手动部署勒索软件，以基础架构的安全性为威胁，迫使受害者交赎金。

3. 攻击者仿冒英国税务及海关总署的页面对英国公民进行网络诈骗

11 月 8 日，据 bleepingcomputer 网站消息，攻击者伪装成英国税务及海关总署（HMRC）通过短信针对英国居民发起了一场高级退税骗局。攻击者使用了多个 HMRC 钓鱼域名和策略，每天都会增加新的域名，来规避旧的域名被垃圾邮件过滤器标记。钓鱼网页不仅细致地模仿 HMRC 的网页界面，而且还

内置了完整的网上银行工作流程。这种诈骗始于发送短信，告知收到信息的人今年已经支付了所谓的“紧急税款”，因此有资格获得退税。

4. 印度杂货电商 BigBasket 遭黑客攻击 2000 万 用户信息被泄

11 月 9 日，Hackernews 消息，援引多家印媒报道，印度最大杂货电商 BigBasket 近期遭受黑客网络攻击，导致大约 2000 万用户的个人数据被泄漏。这些泄漏的信息包括用户的电子邮件地址、密码哈希值、联系方式（移动和手机）、地址、生日、住址和登录 IP 地址等等，这些信息在暗网上以 300 万卢比（约 26.8 万人民币）的价格出售。安全公司 Cybel 在 10 月 30 日发现安全泄露事件之后已经告知了 BigBasket。并且该电子商务平台已向位于班加罗尔（Bangaluru）的网络犯罪小组（Cyber Crime Cell）投诉。该公司正在评估“索赔的违反程度和真实性”。

5. 笔记本电脑制造商仁宝遭高额赎金勒索攻击

11 月 10 日，据 FreeBuf 报道，笔记本电脑制造商仁宝遭网络攻击。仁宝是全球第二大笔记本电脑原始设计制造商（ODM），客户涵盖苹果、惠普、戴尔、联想和宏碁等。媒体根据仁宝员工分享的赎金记录的屏幕快照和攻击勒索票据分析，很大可能是遭遇了勒索软件攻击，幕后黑手则是 DoppelPaymer 勒索软件组织。根据赎金记录中链接的 DoppelPaymerTor 付款网站，勒索软件团伙要求提供 1,100 比特币才能获取解密器。

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：张腾

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315