国家互联网应急中心

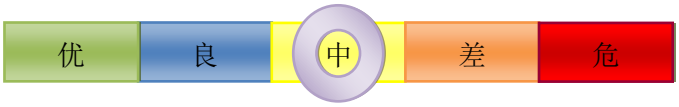
网络安全信息与动态周报

2019 年第 45 期

11 月 4 日-11 月 10 日

CNCERT/CC

本周网络安全基本态势

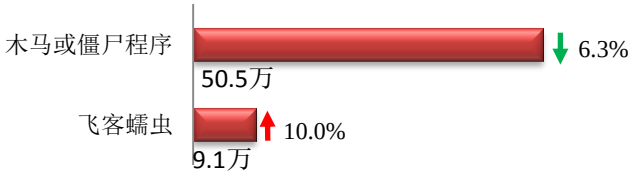


境内感染网络病毒的主机数量	•59.58万	4.1%
境内被篡改网站总数 其中政府网站数量	•6386 •10	3.6% 41.2%
境内被植入后门网站总数 其中政府网站数量	•3365 •47	13.1% 35.6%
针对境内网站的仿冒页面数量	•614	67.4%
新增信息安全漏洞数量 其中高危漏洞数量	•425 •105	11.1% 14.1%

═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

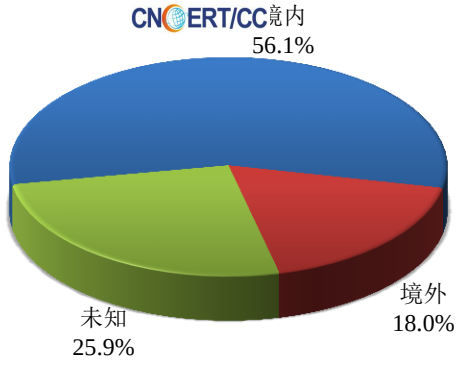
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 59.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 50.5 万以及境内感染飞客（conficker）蠕虫的主机约 9.1 万。

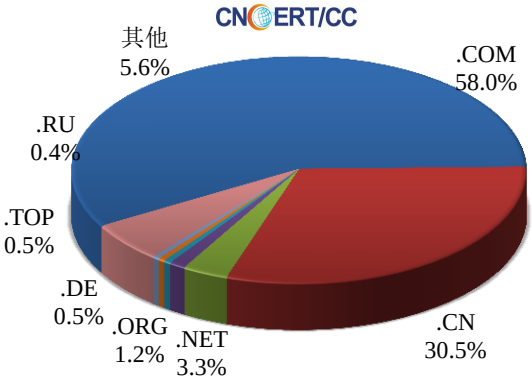


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 2673 个，涉及 IP 地 2464 个。在 2673 个域名中，有 18.0%为境外注册，且顶级域为.com 的约占 58.0%；在 2464 个 IP 中，有约 43.0%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 329 个 IP。

本周放马站点域名注册所属境内外分布
(11/4-11/10)



本周放马站点域名所属顶级域的分布
(11/4-11/10)



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。

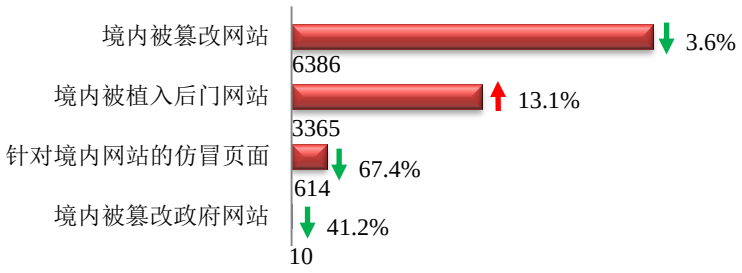
ANVA恶意地址黑名单发布地址

http://www.anva.org.cn/virusAddress/listBlack

中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由中国互联网协会网络与信息安全工作委员会发起、CNCERT 具体组织运作的行业联盟。

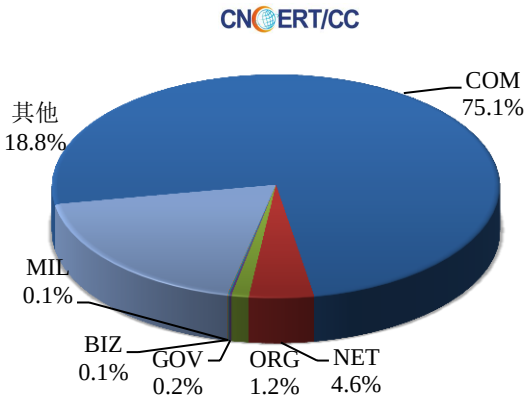
本周网站安全情况

本周 CNCERT 监测发现境内境内被篡改网站数量 6386 个；被植入后门的网站数量为 3365 个；针对境内网站的仿冒页面数量 614 个。

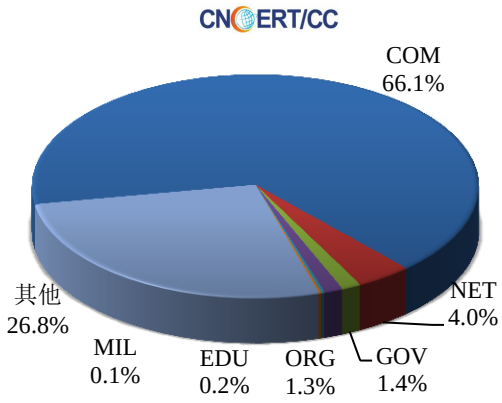


本周境内被篡改政府网站（GOV 类）数量为 10 个（约占境内 0.2%），较上周环比下降了 41.2%；境内被植入后门的政府网站（GOV 类）数量为 47 个（约占境内 1.4%），较上周环比下降 35.6%；针对境内网站的仿冒页面涉及域名 456 个，IP 地址 146 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内篡改网站按类型分布
(11/4-11/10)

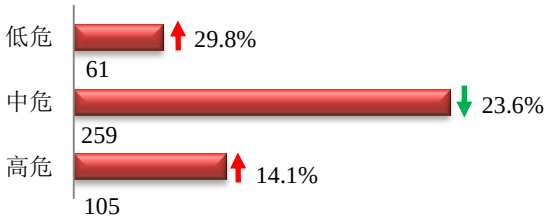


本周我国境内被植入后门网站按类型分布
(11/4-11/10)

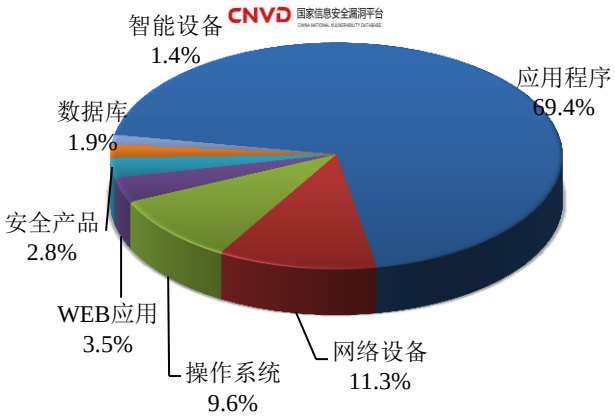


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 425 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类型分布
(11/4-11/10)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是操作系统和 WEB 应用漏洞。

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

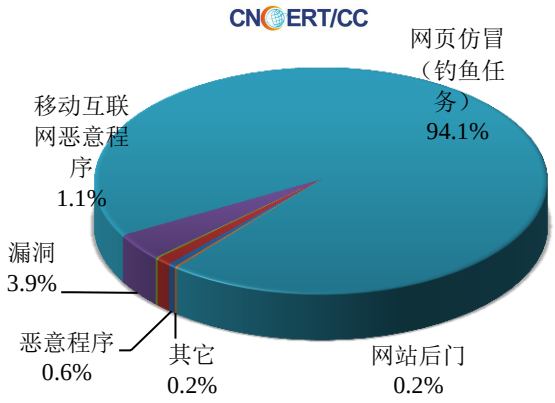
http://www.cnvd.org.cn/webinfo/list?type=4

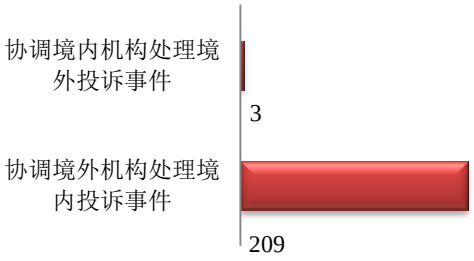
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 542 起，其中跨境网络安全事件 212 起。

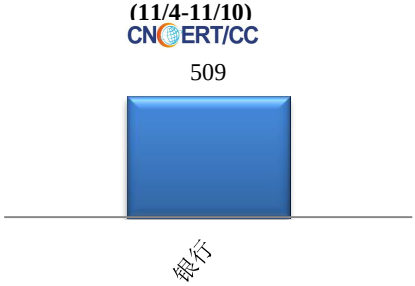
本周CNCERT处理的事件数量按类型分布 (11/4-11/10)



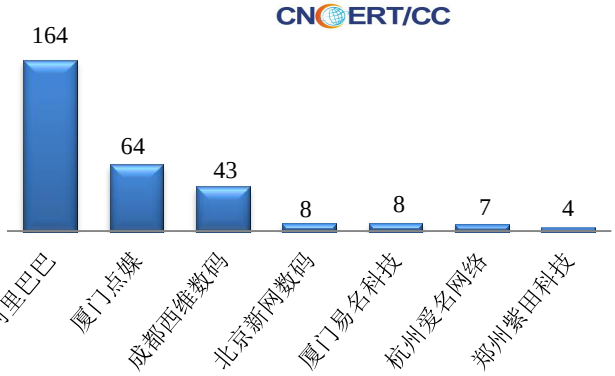


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 509 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，509 起皆为银行仿冒事件。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (11/4-11/10)

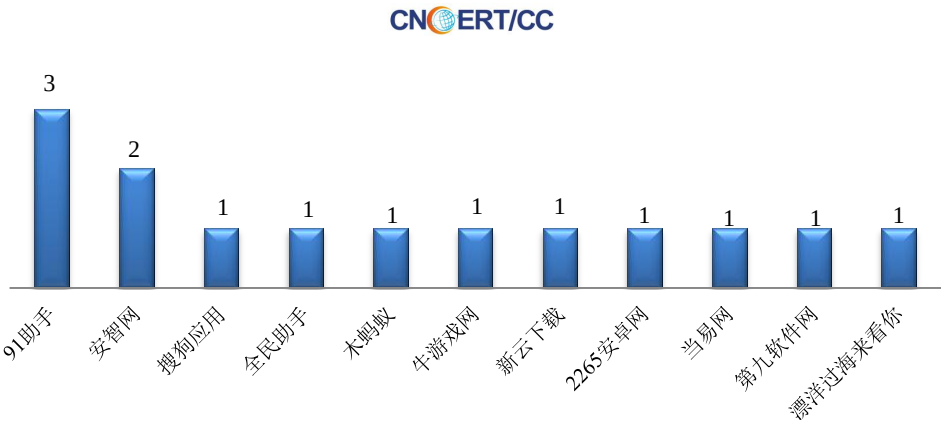


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (11/4-11/10)



本周，CNCERT 协调 11 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 14 个。

本周CNCERT协调手机应用商店处理移动互联网恶意代码事件数量排名
(11/4-11/10)



业界新闻速递

1、 美国防部向海外部署网络人员以收集情报保障 2020 年总统选举

据 cyberscoop 网站消息，美国驻黑山大使馆宣布，五角大楼再次将网络人员派往海外，以收集情报帮助保障 2020 年总统选举免受外国干扰。美军欧洲司令部和网络司令部正在向黑山部署数量不明的防御性网络运营人员，以便在明年美国和黑山共和国大选之前了解网络威胁。美国国务卿迈克·庞培（Mike Pompeo）上个月表示，由于去年的合作所收集的情报，直接导致美国能够抵御最新的俄罗斯恶意软件。俄罗斯黑客此前曾对黑山发起鱼叉式攻击，这可以为美国提供技术数据。去年，美军网络司令部与黑山一起向乌克兰和北马其顿部署了人员，以收集网络威胁情报，为 2018 年中期选举做准备。这些行动被称为“狩猎向前”，黑山是目前正在进行的唯一一次行动，尚不清楚美军网络司令部与哪些其他国家结成伙伴关系开展此行动。今年早些时候，美军网络司令部称正与多个盟友在国外进行部署，但未透露是哪些国家。

2、 西班牙两家公司同天遭勒索软件攻击，引发 WannaCry 级恐慌

11 月 5 日 HackerNews 网站消息，近日，西班牙两家大型公司 Everis（NTT Data Group 旗下的 IT 咨询公司）和 Cadena SER（西班牙最大的无线电网络公司）在同一天内受到勒索软件打击，两家公司都要求员工关闭计算机，并断开网络连接。Everis 在全球 18 个国

家或地区拥有超过 2 万名员工，勒索软件已通过公司的内部网络传播，其他分支也受到了影响。西班牙国家安全局在事件发生后的数小时内发布安全建议，敦促公司改善网络安全措施，并且建议其他受害者向西班牙国家网络安全研究所 INCIBE 寻求帮助。据报道，尽管没有类似 WannaCry 的勒索软件爆发的迹象，但这两个公司感染恶意程序事件对西班牙当地的商业环境产生了重大影响，许多本地公司使用 Everis 软件进行日常活动，有人担心自己被感染，选择关闭程序来检查系统。

3、 美加州下令要求 Facebook 交出涉嫌侵犯用户隐私的相关信息

11 月 6 日 CNBC 消息，美国加州司法部长 Xavier Becerra 表示，Facebook 拒绝遵守要求其提供更多关于对其涉嫌侵犯用户隐私的调查信息的传票。在当地时间周三下午的新闻发布会上，Becerra 谈到了加州对 Facebook 的诉讼，要求该公司交出任何跟隐私和第三方获取用户数据有关的文件，就像在剑桥分析丑闻中做的那样。Becerra 指出，Facebook“没有完全回应”他办公室提出的信息要求，公开这些信息是别无选择。

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 2018 年，CNCERT 与 76 个国家和地区的 233 个组织建立了“CNCERT 国际合作伙伴”关系。

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