国家互联网应急中心

网络安全信息与动态周报

2019 年第 7 期

2 月 11 日-2 月 17 日

CNCERT/CC

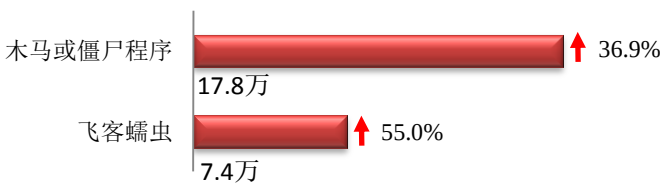
本周网络安全基本态势

境内感染网络病毒的主机数量	•25.2万	↑36.9%
境内被篡改网站总数 其中政府网站数量	•490 •36	↓19.4% ↓2.7%
境内被植入后门网站总数 其中政府网站数量	•396	↑11.9%
针对境内网站的仿冒页面数量	•795	↑127.1%
新增信息安全漏洞数量 其中高危漏洞数量	•218 •62	↑6.3% ↑21.6%

=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

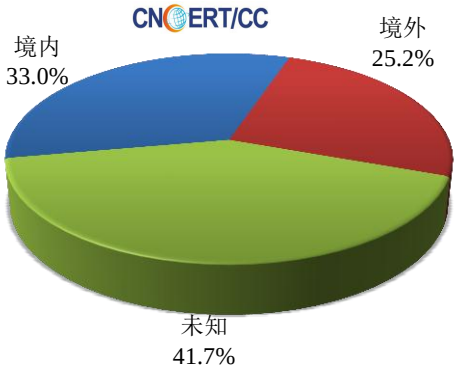
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 25.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 17.8 万以及境内感染飞客（conficker）蠕虫的主机约 7.4 万。

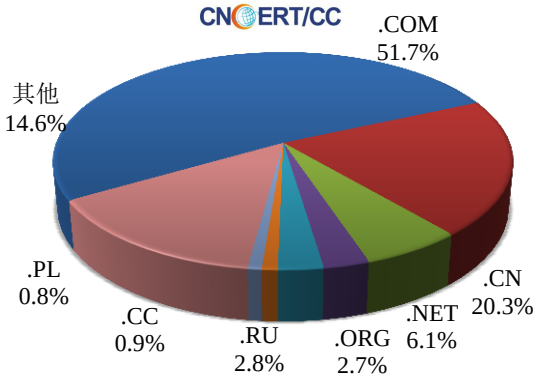


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1909 个，涉及 IP 地址 3763 个。在 1909 个域名中，有 25.2%为境外注册，且顶级域为.com 的约占 51.7%；在 3763 个 IP 中，有约 55.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 383 个 IP。

本周放马站点域名注册所属境内外分布
(2/11-2/17)



本周放马站点域名所属顶级域的分布
(2/11-2/17)



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。

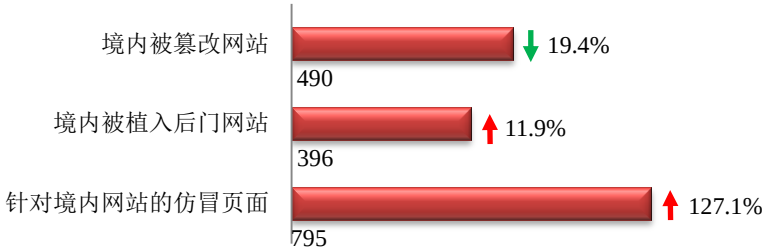
ANVA恶意地址黑名单发布地址

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。

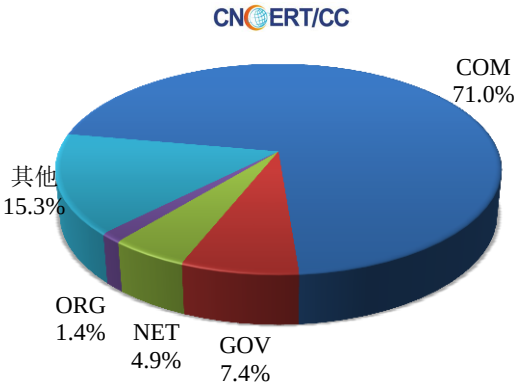
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 490 个；境内被植入后门的网站数量为 396 个；针对境内网站的仿冒页面数量 795 个。

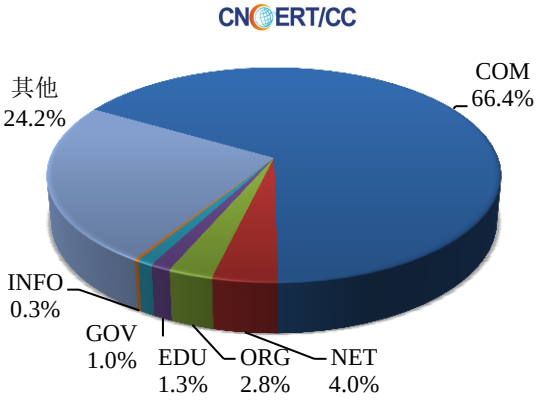


本周境内被篡改政府网站（GOV 类）数量为 36 个（约占境内 7.3%），较上周环比下降了 2.7%；境内被植入后门的政府网站（GOV 类）数量为 4 个（约占境内 1.0%）；针对境内网站的仿冒页面涉及域名 249 个，IP 地址 132 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(2/11-2/17)

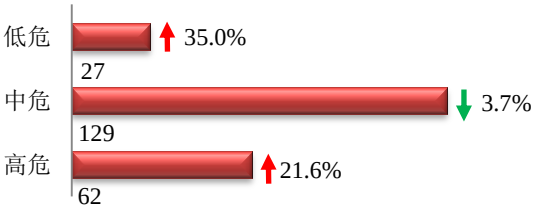


本周我国境内被植入后门网站按类型分布
(2/11-2/17)

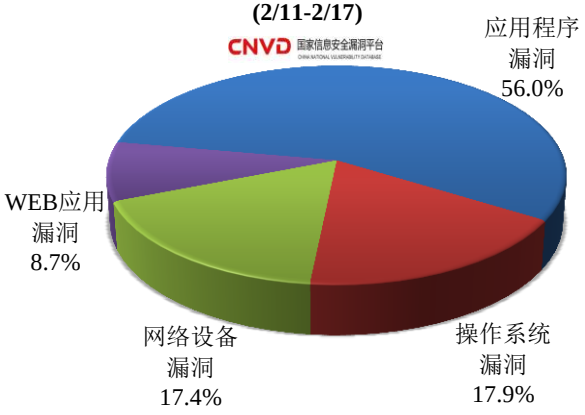


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 218 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
(2/11-2/17)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是操作系统漏洞和网络设备漏洞。

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

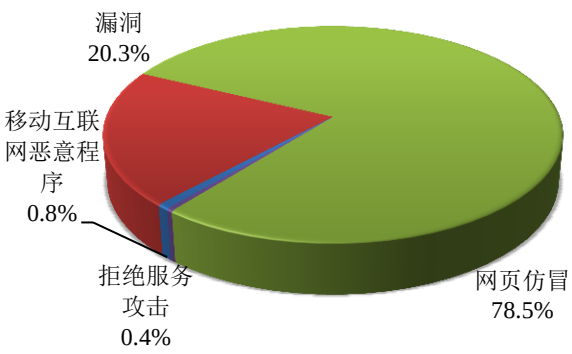
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

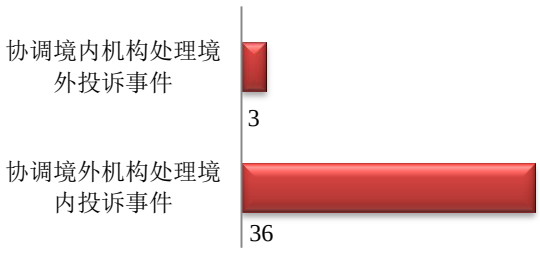
本周事件处理情况

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 256 起，其中跨境网络安全事件 39 起。

本周CNCERT处理的事件数量按类型分布 (2/11-2/17)

CNCERT/CC

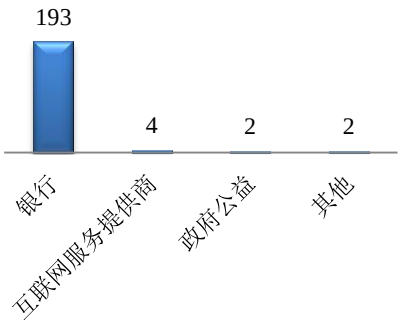




本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 201 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 193 起和互联网服务提供商仿冒事件 4 起。

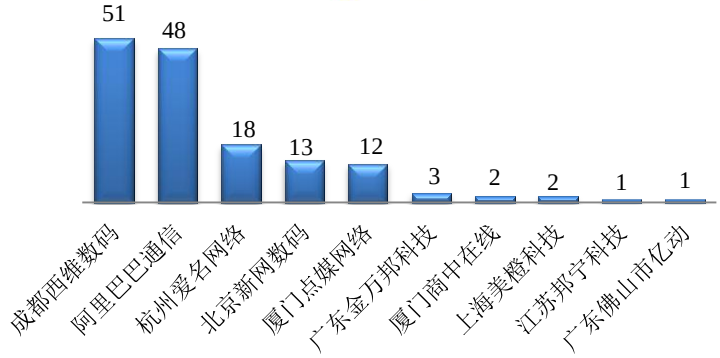
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (2/11-2/17)

CNCERT/CC



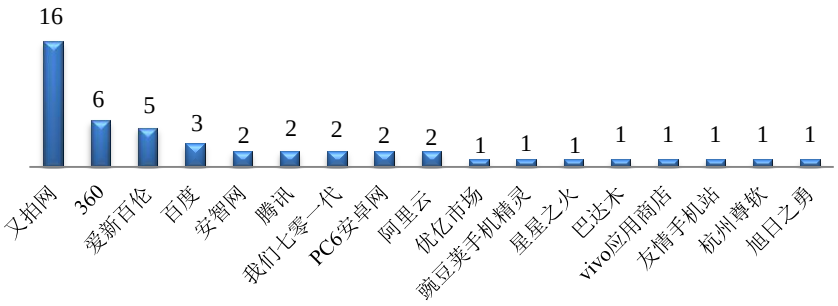
本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (2/11-2/17)

CNCERT/CC



本周，CNCERT 协调 17 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 48 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
(2/11-2/17)
CNCERT/CC



业界新闻速递

1、特朗普政府颁布行政令 要求优先发展人工智能

新浪科技 2 月 12 日消息 美国总统特朗普 11 日签署行政令，要求联邦政府机构配置更多资源和投资用于人工智能(AI)的研究、推广和培训。根据美国 AI 倡议(American AI Initiative)，政府要求各部门将 AI 研发投资作为重点、增加联邦数据和模型与 AI 研究之间的渠道，并使雇员做好准备以适应 AI 时代。这一倡议旨在确保美国维持在 AI 研发及相关领域的优势，如先进制造业和量子计算。

2、德国将帮助北约解决网络安全方面的问题

E 安全 02 月 16 日消息 德国宣布将与北约分享其网络战能力，以保护联盟成员国免受黑客攻击和电子战的伤害。北约在 2016 年华沙峰会上正式承认网络空间为军事行动领域。一旦发生严重的网络攻击，北约会使用常规武器作出反击。这表明互联网是一个新的战场。民族国家的黑客行为和网络罪犯实施的攻击越来越频繁，破坏性也越来越强，让北约不得不加强网络能力。联盟的目标是扩大北约网络范围，使盟国能够提高网络能力，并在威胁和实践方面共享信息。

3、美国反间谍特工帮助伊朗向美国发射网络炸弹

E 安全 02 月 15 日消息 美国检察官于宣布对一名前美国反间谍特工提起公诉，罪名是帮助伊朗对其前同事实施网络攻击，同时也起诉了四名伊朗公民实施了与之相关的计算机犯罪。美国司法部称，39 岁的前美国空军情报特工 Monica Elfriede Witt 于 2013 年叛逃至伊朗，并向伊朗情报部门提供机密信息，协助伊朗编写关于美国情报人员的背景研究报告，以便对他们进行网络攻击。起诉书中提到的四名伊朗人曾在伊朗革命卫队工作，曾在 2014 年和 2015 年对美国情报人员发动网络攻击。美国已对 Witt 和她的同谋发出了逮捕令，但他们目前仍

逍遥法外。这个团体利用一名情报人员 Facebook 上的照片创建了一个冒名 Facebook 账户，与其他情报人员建立好友关系，诱使他们点击带有恶意文件的共享链接，但起诉书中没有提到攻击者是否成功破坏了目标系统。

4、VFEmail 遭黑客攻击 美国区所有数据被删除且无法恢复

cnBeta.COM02 月 13 日消息 总部位于美国密尔沃基的电子邮件提供商 VFEmail 遭遇了一场“灾难性”攻击，导致其美国境内服务器上主要和备份系统上的所有数据被破坏。VFEmail 所有者 Rick Romero 近期发现有黑客试图系统性破坏公司的服务硬盘，其中包括备份和冗余。根据该电子邮件服务提供商在官网上发布的通告，其美国服务器上的“所有数据”已经完全消失，而且似乎无法恢复。

5、马耳他银行遭遇网络攻击，黑客将资金转移到国外

E 安全 2 月 15 日消息 有黑客侵入马耳他的瓦莱塔银行（Bank of Valletta）系统并将资金转移到海外，该银行于 2 月 13 日关闭了所有业务。瓦莱塔银行的业务交易量大约是马耳他银行业业务交易量的一半。黑客向英国、美国、捷克和香港的银行转移了总计 1300 万欧元（大约 1470 万美元）。目前这些资金已被追踪，瓦莱塔银行正试图扭转这个局面。攻击在 2 月 13 日银行开始营业后不久后被发现，当时银行正在进行国际贸易协调。国家安全部门通知该行，银行受到了网络攻击。为了将风险降至最低并重新评估银行系统，瓦莱塔银行暂停了运营，关闭了位于地中海岛屿的分支机构、ATM 机和网站。

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 2017 年，CNCERT 与 72 个国家和地区的 211 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：王小群

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158