国家互联网应急中心

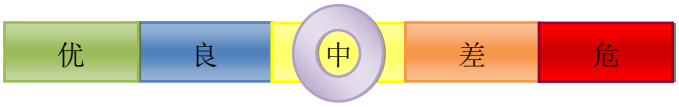
网络安全信息与动态周报

2019 年第 48 期

11 月 25 日-12 月 1 日

CNCERT/CC

本周网络安全基本态势

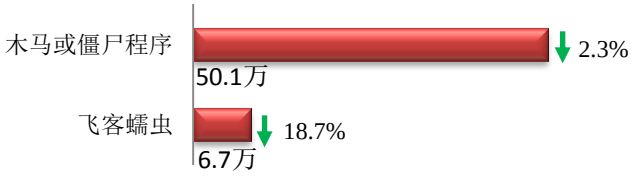


境内感染网络病毒的主机数量	•56.83万	↓4.6%
境内被篡改网站总数 其中政府网站数量	•1427 •5	↓77.4% ↓79.2%
境内被植入后门网站总数 其中政府网站数量	•3631 •37	↑3.9% ↓15.9%
针对境内网站的仿冒页面数量	•690	↑42.3%
新增信息安全漏洞数量 其中高危漏洞数量	•402 •91	↓18.6% ↓38.1%

═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

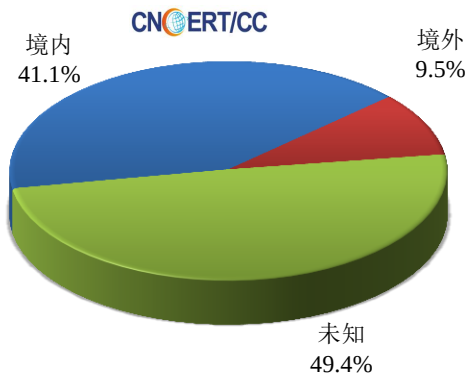
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 56.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 50.1 万以及境内感染飞客（conficker）蠕虫的主机约 6.7 万。

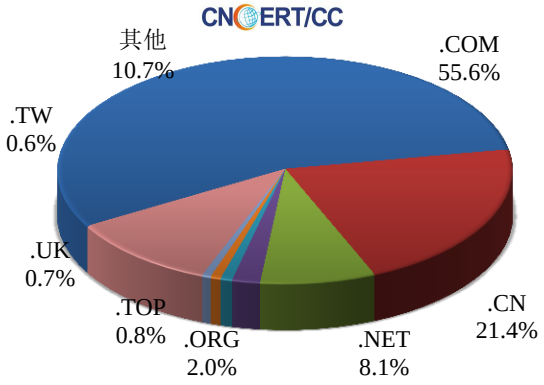


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 959 个，涉及 IP 地址 2111 个。在 959 个域名中，有 9.5%为境外注册，且顶级域为.com 的约占 55.6%；在 2111 个 IP 中，有约 36.0%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 299 个 IP。

本周放马站点域名注册所属境内外分布
(11/25-12/01)



本周放马站点域名所属顶级域的分布
(11/25-12/01)



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。

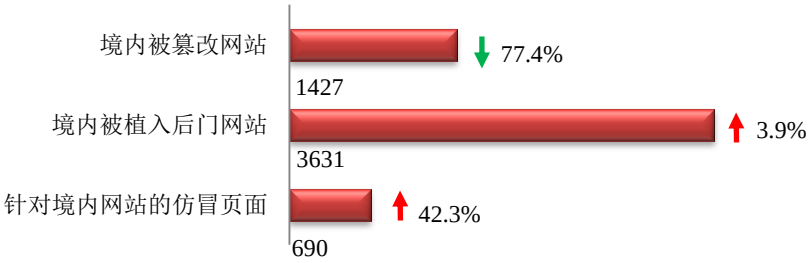
ANVA恶意地址黑名单发布地址

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。

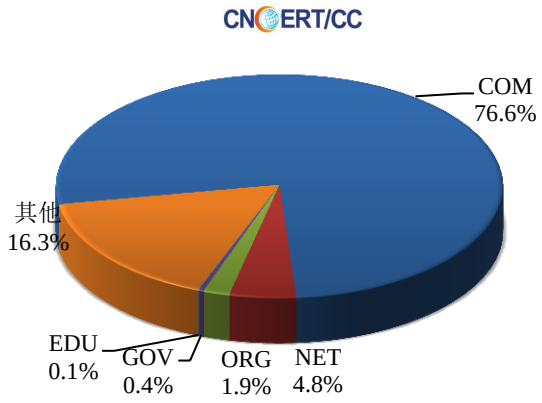
本周网站安全情况

本周 CNCERT 监测发现境内境内被篡改网站数量 1427 个；被植入后门的网站数量为 3631 个；针对境内网站的仿冒页面数量 690 个。

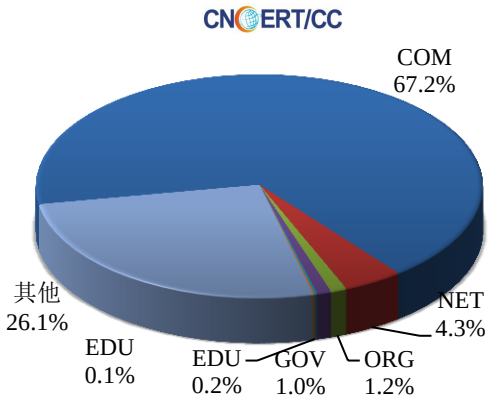


本周境内被篡改政府网站（GOV 类）数量为 5 个（约占境内 0.4%），较上周环比下降了 79.2%；境内被植入后门的政府网站（GOV 类）数量为 37 个（约占境内 1.0%），较上周环比下降了 15.9%。

本周我国境内篡改网站按类型分布
(11/25-12/01)

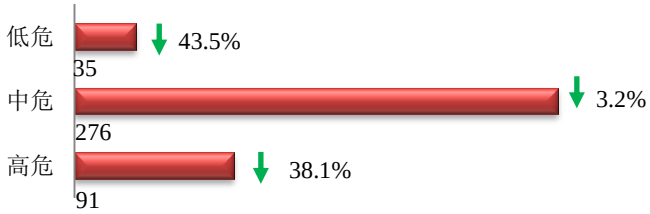


本周我国境内被植入后门网站按类型分布
(11/25-12/01)

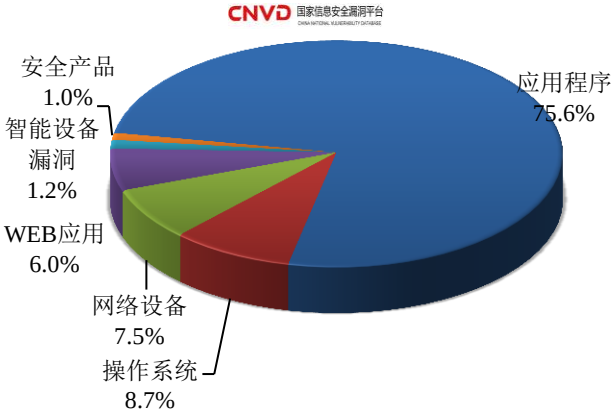


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 402 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
(11/25-12/01)



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

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

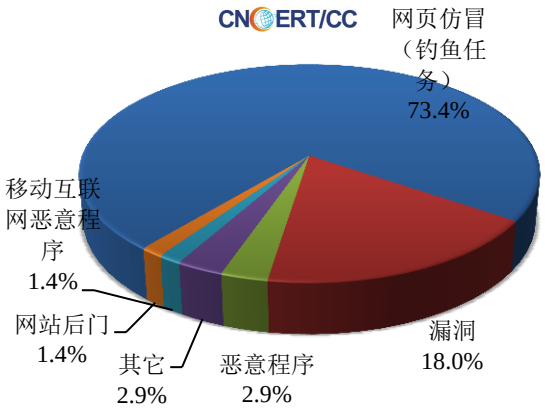
http://www.cnvd.org.cn/webinfo/list?type=4

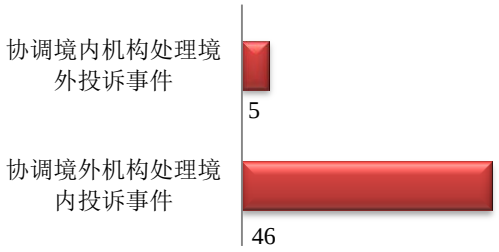
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 139 起，其中跨境网络安全事件 51 起。

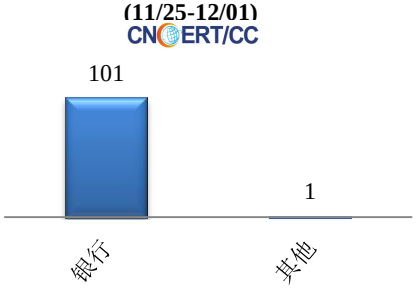
本周CNCERT处理的事件数量按类型分布 (11/25-12/01)



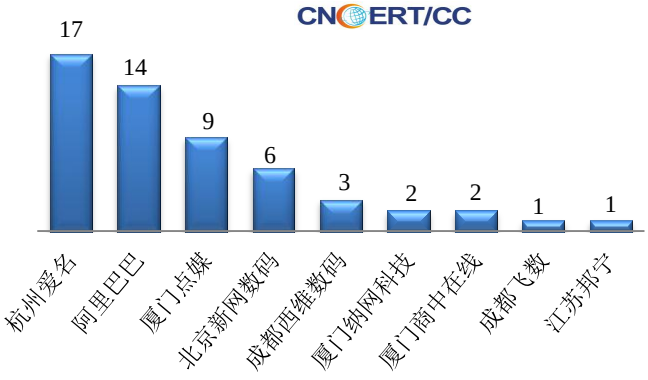


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 102 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包括银行仿冒事件 101 起和其他事件 1 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (11/25-12/01)

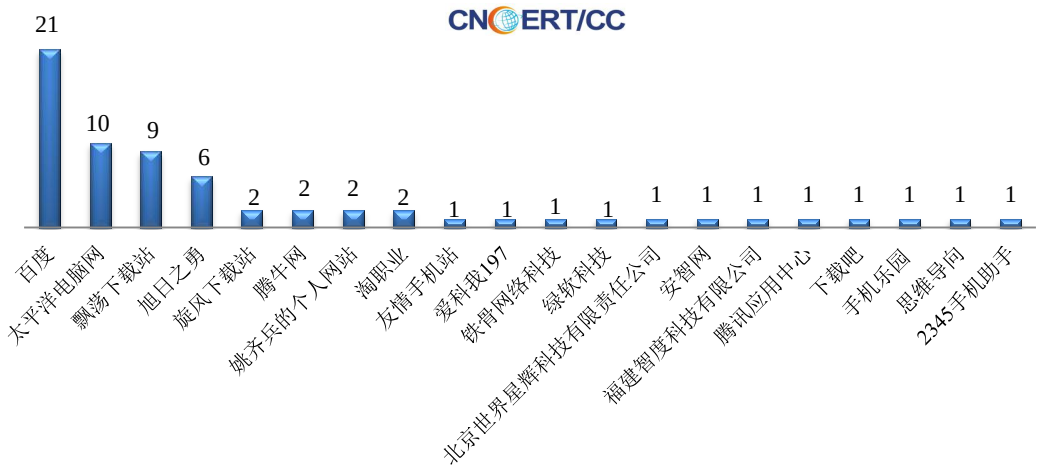


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (11/25-12/01)



本周，CNCERT 协调 20 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 66 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
(11/25-12/01)



业界新闻速递

1、 三部门联合印发《网络音视频信息服务管理规定》

11 月 29 日，国家互联网信息办公室、文化和旅游部、国家广播电视总局联合印发《网络音视频信息服务管理规定》，促进网络音视频信息服务健康有序发展。规定对网络音视频信息服务提供者提出要求，应当依法取得法律、行政法规规定的相关资质；应当建立健全用户注册、信息发布审核、信息安全管理等制度；应当依照网络安全法的规定，对用户进行基于组织机构代码、身份证件号码、移动电话号码等方式的真实身份信息认证。同时还要求，任何组织和个人不得利用网络音视频信息服务以及相关信息技术从事法律法规禁止的活动，侵害他人合法权益。规定对基于深度学习、虚拟现实等的新技术新应用制作、发布、传播音视频信息也作出了相关要求。规定自 2020 年 1 月 1 日起施行。

2、 欧洲数据保护委员会通过《一般数据保护条例》相关准则

11 月 26 日，据英国“Mondaq（曼达克）”网站消息，11 月 12 日,欧洲数据保护委员会（EDPB）在第 15 次全体会议上通过《一般数据保护条例》领土范围的最终准则。该准则旨为数据保护机构在评估管理者或处理者的处理是否属于《一般数据保护条例》的范围，欧洲数据保护委员会目前正在考虑发展国际合作机制。

3、 万维网之父发起拯救互联网计划：确保始终惠及人类

11 月 25 日，据美国消费者新闻与商业频道（CNBC）报道，万维网之父蒂姆·伯纳斯-李（Sir Tim Berners-Lee）公布了一项名为《互联网契约》（Contract for the Web）的拯救网络的全球计划，呼吁政府和企业能够阻止对互联网的滥用，保护互联网免受政治操纵、假新闻、侵犯隐私等其他威胁。《互联网契约》由 80 个组织进行了一年多的研究，概述了 9 项保护互联网的中心原则，针对政府、企业和个人的原则各 3 个。支持《契约》的机构必须表现出他们正在执行这些原则，并致力于解决更棘手的问题。《契约》要求，政府尽一切努力，保证想要上网的所有人能够连接上网，并尊重其隐私。人们应有权访问保存他们个人数据的任何地方。

4、 开曼国家银行已证实被黑客入侵：2.21TB 数据惨遭泄露

11 月 21 日，据 Freebuf 国际安全智库消息，开曼国家银行发生了严重的数据泄露事故，多达 2TB 的机密数据遭到黑客窃取。开曼国家银行位于开曼群岛，是全球知名的避税天堂。11 月 15 日，一自称 Phineas Fisher 的黑客或黑客组织公开发表宣言称，他们已经入侵了开曼国家银行窃取了数十万美元，并高调地表示在数字时代抢劫银行是一种非暴力、低风险、高回报的行动。随后，该黑客还通过网站 Distributed Denial of Secrets 公开了从开曼国家银行窃取到的 2.21TB 数据。此次事故泄露了该银行的 3800 多个公司、信托和个人帐户的详细财务信息。根据已知的信息，受害者多来自马恩岛、塞浦路斯、英国和开曼群岛。11 月 18 日，开曼国家银行公开发布一份声明，证实其数据信息遭到入侵，该银行并没有明确提到 Phineas Fisher，而只是说是此次事件的受害者。

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：李志辉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315