国家互联网应急中心

网络安全信息与动态周报

2017 年第 47 期

11 月 13 日-11 月 19 日

CNCERT/CC

本周网络安全基本态势

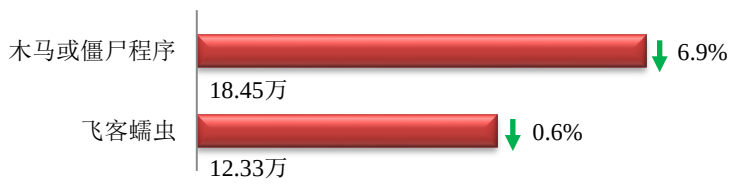
境内感染网络病毒的主机数量	• 30.78万	↓ 4.5%
境内被篡改网站总数 其中政府网站数量	• 1587 • 54	↓ 4.7% ↑ 1.9%
境内被植入后门网站总数 其中政府网站数量	• 792 • 16	↑ 0.9% ↓ 44.8%
针对境内网站的仿冒页面数量	• 395	↑ 13.8%
新增信息安全漏洞数量 其中高危漏洞数量	• 568 • 204	↑ 6.4% ↑ 33.3%

v

= 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

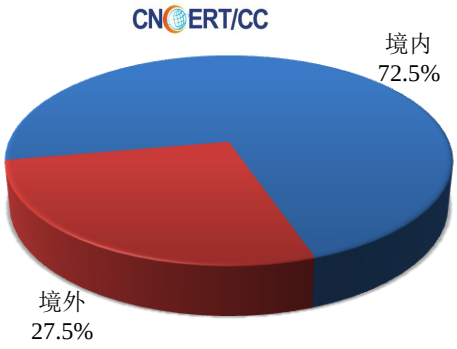
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 30.78 万个，其中包括境内被木马或被僵尸程序控制的主机约 18.45 万以及境内感染飞客（conficker）蠕虫的主机约 12.33 万。

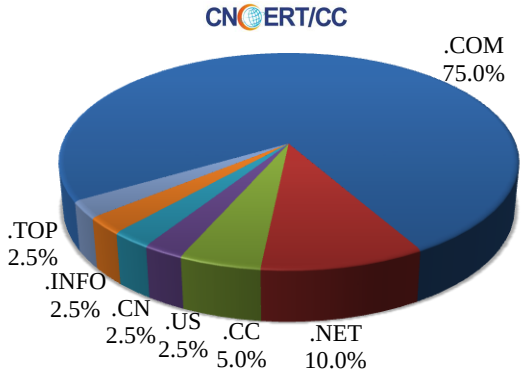


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 40 个，涉及 IP 地址 215 个。在 40 个域名中，有 27.5%为境外注册，且顶级域为.com 的约占 75.0%；在 215 个 IP 中，有约 31.6%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 1 个 IP。

本周放马站点域名注册所属境内外分布
(11/13-11/19)



本周放马站点域名所属顶级域的分布
(11/13-11/19)



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。

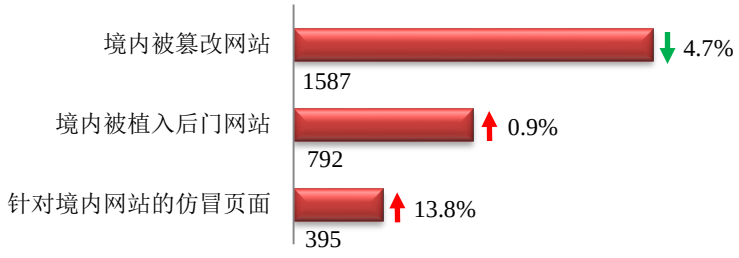
ANVA恶意地址黑名单发布地址

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。

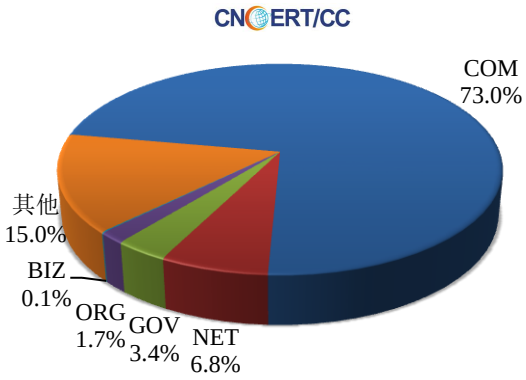
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1587 个；境内被植入后门的网站数量为 792 个；针对境内网站的仿冒页面数量为 395。

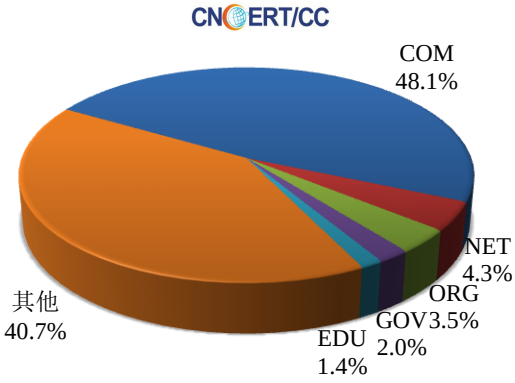


本周境内被篡改政府网站（GOV 类）数量为 54 个（约占境内 3.4%），较上周环比上升了 1.9%；境内被植入后门的政府网站（GOV 类）数量为 16 个（约占境内 2.0%），较上周环比下降了 44.8%；针对境内网站的仿冒页面涉及域名 347 个，IP 地址 145 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(11/13-11/19)

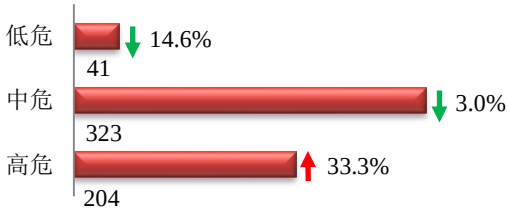


本周我国境内被植入后门网站按类型分布
(11/13-11/19)

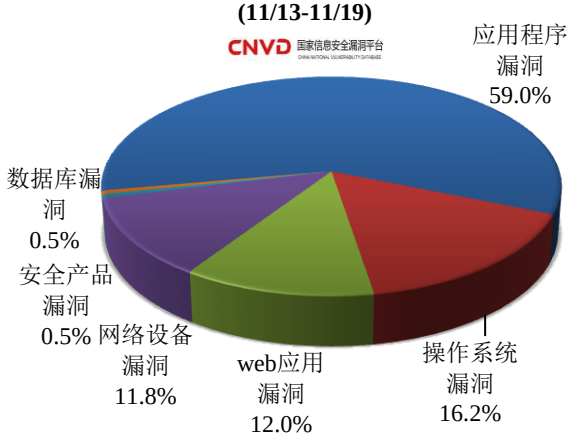


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 568 个，信息安全漏洞威胁整体评价级别为高。



本周CNVD收录漏洞按影响对象类型分布
(11/13-11/19)



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 web 应用漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

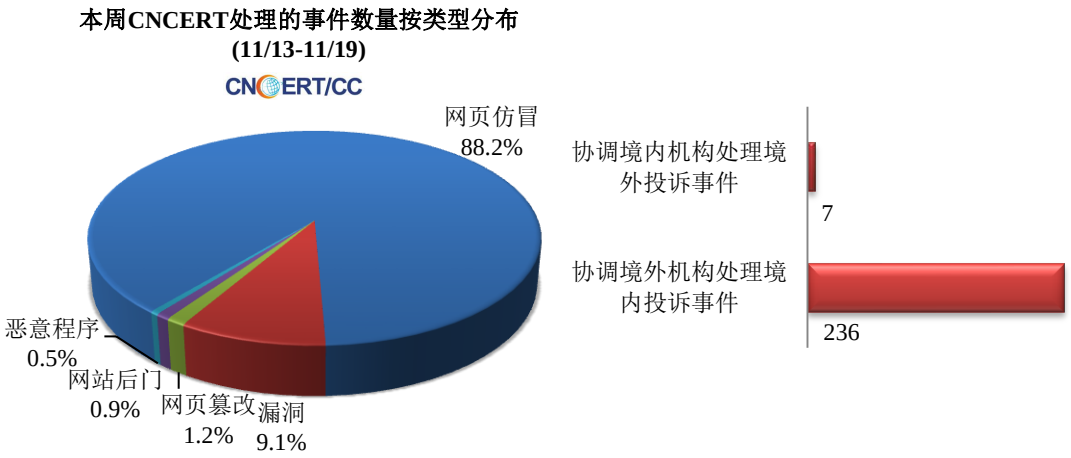
CNVD漏洞周报发布地址

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。

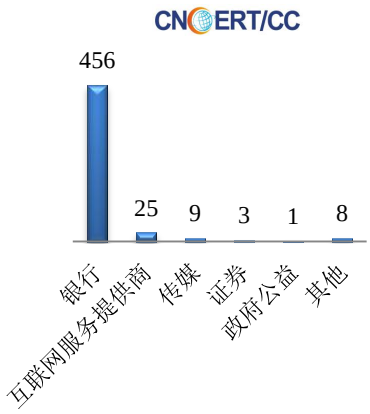
本周事件处理情况

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 569 起，其中跨境网络安全事件 243 起。

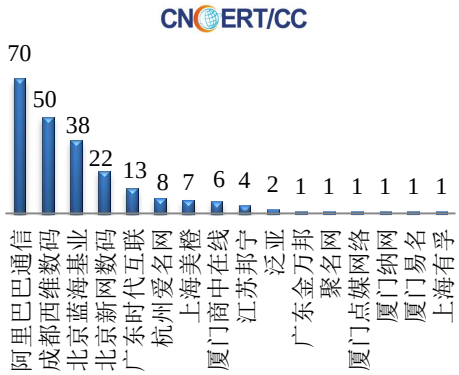


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 502 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 456 起和互联网服务提供商仿冒事件 25 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(11/13-11/19)

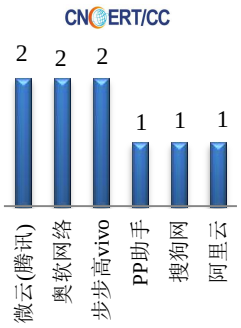


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (11/13-11/19)



本周，CNCERT 协调 6 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 9 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 (11/13-11/19)



业界新闻速递

1、特朗普政府发布新 VEP 机制，以防国家组织私自“库存”漏洞

HackerNews.cc11 月 17 日消息 据外媒 ZDNet 报道，美国白宫网络安全协调员罗伯·乔伊斯（Rob Joyce）于本周三在华盛顿特区出席活动时宣布，特朗普政府已发布一套非机密规则来更新 Vulnerabilities Equities Process（VEP）机制，以平息舆论中政府大量“库存”漏洞发起黑客攻击的虚假谣言。VEP 是奥巴马就任时所发布的一套复杂而重要的保密机制，决定了美国政府在发现漏洞后衡量是否秘密通知受影响的科技公司，并提醒其产品或服务存在漏洞，以便黑客入侵前迅速修复。今年早些时候，神秘黑客组织“影子经纪人”（Shadow Brokers）通过窃取 NSA 存储的漏洞开展了大规模勒索软件 WannaCry 攻击活动，感染了全球 150 多个国家逾 30 万台电脑。随后，特朗普政府遭到指责并在 NSA 黑客工具被窃不到一年内更新了该份报告。知情人士透露，这一举措能够防止政府私自储存漏洞、黑客工具或网络武器，并被认为是美国政府所公布的一项极其罕见的行为，因为该机制自奥巴马执政以来一直处于保密状态。

2、乌克兰将实施网络安全法

凤凰网 11 月 14 日消息 乌克兰总统波罗申科近日签署《关于保障乌克兰网络安全的基本原则法》（以下简称《网络安全法》），该法律将于正式公布之日起六个月后生效。乌克兰总统网站发布的消息称，乌克兰最高拉达（议会）10 月 5 日通过了《网络安全法》，该法律将建立起乌国家网络安全的基本体系，通过对国有、私营部门以及公民社会采取组织行政和技术措施，将政治、社会、经济和信息关系进行整合。《网络安全法》是为确保个人、公民、社会和国家的切身利益，维护网络空间中的乌克兰国家利益，保障国家机关、企业、机构、组织、个人的权利和责任，为保障协调上述类别开展活动的基本原则等提供法律和组织基础。另外，该法律还对网络安全领域的一些基本术语进行了定义，例如“网络安全”“网络攻击”“网络威胁”“网络间谍行为”“网络恐怖主义”等。乌克兰《网络安全法》还定义了网络防御的主要对象，包括通讯系统和关键基础设施、国家网络安全保障原则以及国家网络安全体系。根据该法律，乌克兰总统将负责协调乌克兰国家安全与国防委员会管理网络安全问题。该法律允许在国家主导下与私营部门和公民社会密切合作，采取综合措施，为乌克兰关键基础设施提供网络防御保障。

3、印度奥里萨邦网络犯罪事件激增，政府新设网络警察局

E 安全 11 月 15 日消息 根据《印度时报》在本周一发表的报道，在印度奥里萨邦涉及网络犯罪的案件正以迅猛的态势上升。奥里萨邦警方刑事部门的一位高级官员 Santosh Upadhaya 说：“我们将在周二组织一个为期两天的网络安全调查计划，对所有隶属于奥里萨邦的警察局的警务人员进行调查并进行培训，以提高他们破解重大网络犯罪的能力。”奥里萨邦政府在前段时间正式宣布将在贝兰普尔、森伯尔布尔和鲁吉拉设立网络警察局，而最近奥里萨邦政府再次决定将新增另外三个城市——布巴内斯瓦尔、科拉普特和巴拉索尔，专门负责处理与网络有关的犯罪案件。

4、荷兰央行将建黑客小组攻击本国银行 以提升防御能力

凤凰网 11 月 14 日消息 据路透消息，荷兰媒体 Het Financieele Dagblad 周二称，荷兰央行（DNB）将设立网络安全专家及黑客小组，攻击本国金融基础设施，以测试并提升其防御性能。该央行支付与基础设施部门主管 Petra Hielkema 在接受该报采访时表示，新成立的团队会对银行、市场以及结算所进行秘密攻击。荷兰央行将在周二稍晚公布该计划的基本规则。

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。截止 2016 年，CNCERT 与 69 个国家和地区的 185 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：顾笑南

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158