国家互联网应急中心

网络安全信息与动态周报

2017 年第 48 期

11 月 20 日-11 月 26 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	•28.5万	7.3%
境内被篡改网站总数 其中政府网站数量	•1343 •43	15.4% 20.4%
境内被植入后门网站总数 其中政府网站数量	•699 •10	11.7% 37.5%
针对境内网站的仿冒页面数量	•366	7.3%
新增信息安全漏洞数量 其中高危漏洞数量	•277 •71	51.2% 65.2%

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

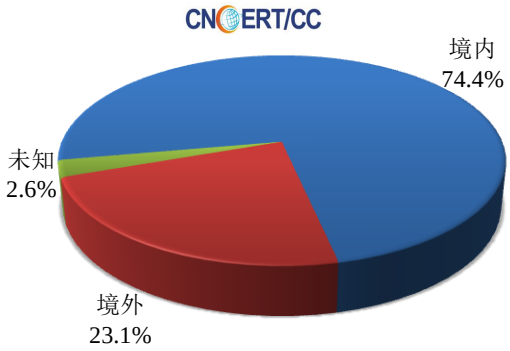
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 28.5 万个，其中包括境内被木马或被僵尸程序控制的主机约 16.2 万以及境内感染飞客（conficker）蠕虫的主机约 12.3 万。

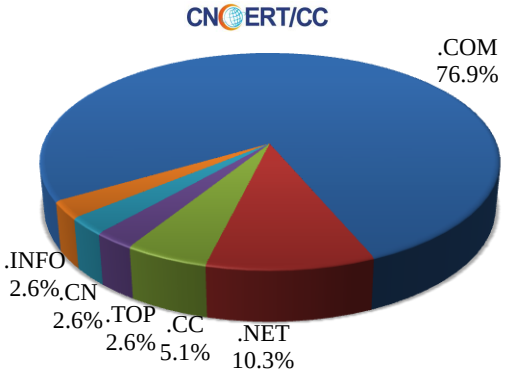
=

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 39 个，涉及 IP 地址 206 个。在 39 个域名中，有 23.1%为境外注册，且顶级域为.com 的约占 76.9%；在 206 个 IP 中，有约 27.7%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 2 个 IP。

本周放马站点域名注册所属境内外分布
(11/20-11/26)



本周放马站点域名所属顶级域的分布
(11/20-11/26)



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。

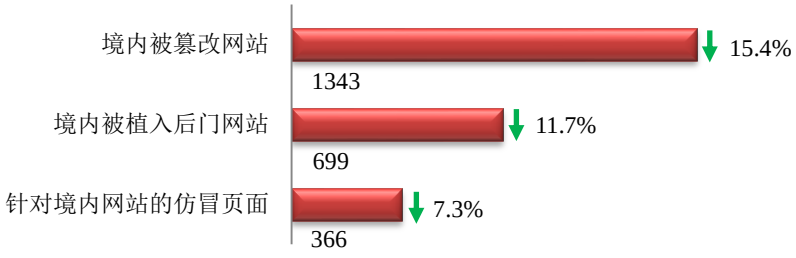
ANVA恶意地址黑名单发布地址

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。

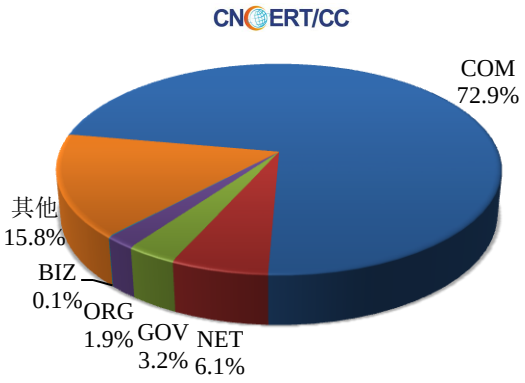
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1343 个；境内被植入后门的网站数量为 699 个；针对境内网站的仿冒页面数量为 366。

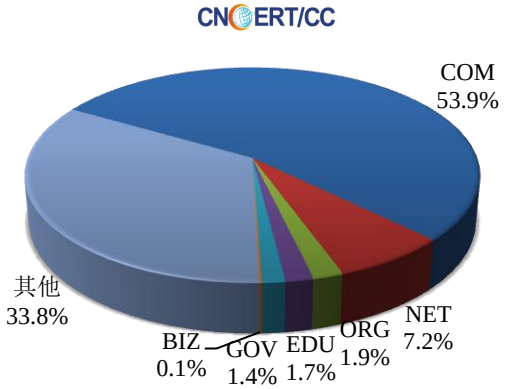


本周境内被篡改政府网站（GOV 类）数量为 43 个（约占境内 3.2%），较上周环比下降了 20.4%；境内被植入后门的政府网站（GOV 类）数量为 10 个（约占境内 1.4%），较上周环比下降了 37.5%；针对境内网站的仿冒页面涉及域名 315 个，IP 地址 124 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(11/20-11/26)

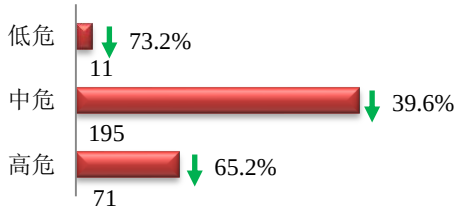


本周我国境内被植入后门网站按类型分布
(11/20-11/26)

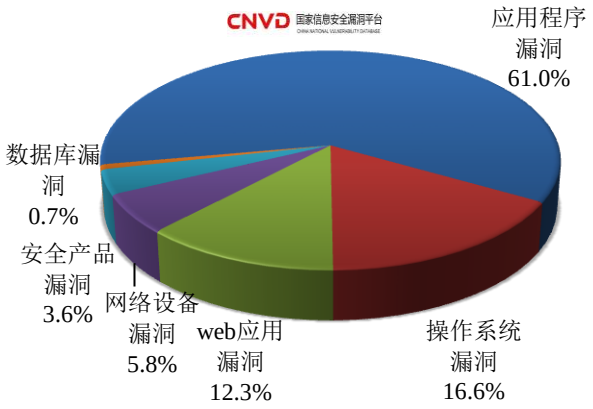


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 277 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
(11/20-11/26)



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。

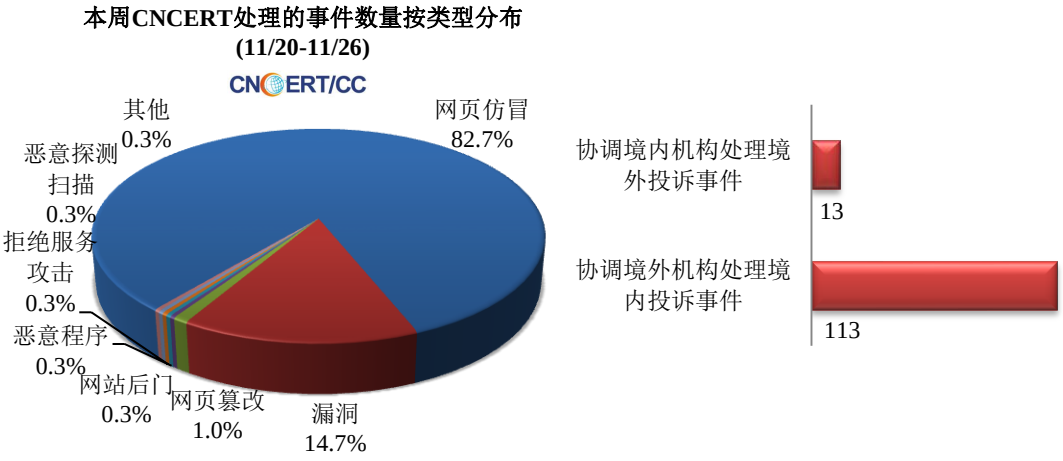
CNVD漏洞周报发布地址

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。

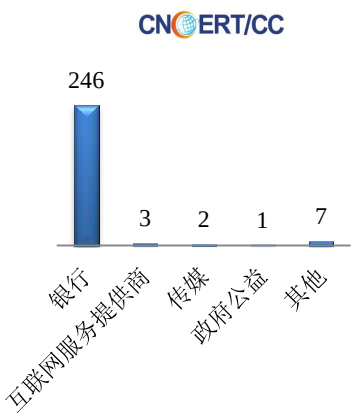
本周事件处理情况

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 313 起，其中跨境网络安全事件 126 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 259 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 246 起和互联网服务提供商仿冒事件 3 起。

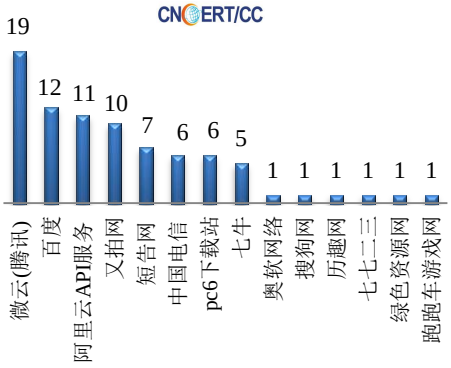
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(11/20-11/26)



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 (11/20-11/26)

本周，CNCERT 协调 14 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 82 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 (11/20-11/26)



业界新闻速递

1、工信部明确公共互联网网络安全突发事件分级预警、应急

新华网 11 月 23 日消息 11 月 23 日从工信部获悉，工信部已印发《公共互联网网络安全突发事件应急预案》，明确了事件分级、监测预警、应急处置、预防与应急准备、保障措施等内容。预案自印发之日起实施。工信部根据社会影响范围和危害程度，将公共互联网网络安全突发事件分为四级：特别重大事件、重大事件、较大事件、一般事件。其中，全国范围大量互联网用户无法正常上网，.CN 国家顶级域名系统解析效率大幅下降，1 亿以上互联网用户信息泄露，网络病毒在全国范围大面积爆发，其他造成或可能造成特别重大危害或影响的网络安全事件为特别重大网络安全事件。工信部要求基础电信企业、域名机构、互联网企业、网络安全专业机构、网络安全企业通过多种途径监测和收集漏洞、病毒、网络攻击最新动向等网络安全隐患和预警信息，对发生突发事件的可能性及其可能造成的影响进行分析评估。认为可能发生特别重大或重大突发事件的，应当立即报告。与此同时，工信部建立公共互联网网络突发事件预警制度，按照紧急程度、发展态势和可能造成的危害程度，

将公共互联网网络突发事件预警等级分为四级，由高到低依次用红色、橙色、黄色和蓝色标示。面向社会发布预警信息有网站、短信、微信等多种形式。

2、欧盟将为遭遇严重网络攻击的成员国提供军事援助

E 安全 11 月 23 日消息 欧盟即将批准修改共同防御规则，将允许遭受网络攻击的成员国向其它国家寻求军事援助。新规则将意味着特别严重的网络事件或危及都可能会是成员国寻求互相帮助的充分动机。这是参考了《里斯本条约》的现有条款，其要求欧盟成员国在其它成员国遭遇恐怖袭击、自然灾害或人为灾难时提供援助。长达 18 页的共同防御规则将在当地时间周一通过。规则并未提及俄罗斯。据消息人士透露，许多网络攻击来自俄罗斯和朝鲜，但强调这并不意味着是国家支持型黑客所为。通过这些新变化，欧盟将步北约（NATO）后尘。北约也认为网络攻击是盟国启用互助条款的充分理由。欧盟也希望阻止第三方干涉内部事务，因此修改“防御协议”，纳入欧盟委员会的建议，允许通过限制性措施避免遭遇网络攻击活动并予以响应，其中提及可能会对开展破坏活动的国家实施制裁。但事实上，要证明政府是网络攻击的幕后黑手几乎不太可能。此外，任何制裁都需要成员国达成一致意见，且只有在有明显证据的情况下才能采用。

3、FCC 将禁止美各州及地方政府制定自己的网络中立法

C114 中国通信网 11 月 23 日消息 据外媒 theverge 报道，在 FCC 开始对网络中立开始进行攻击并打算将其废除之后，美国的一些城市和州开始寻求制定自己的网络中立法。然而不幸的是，FCC 将不会让这样的事情发生：在其最新公布的网络中立废除法律提案中，该委员会打算利用其权力禁止各州及地方政府制定网络中立监管条例。按照 FCC 的计划，各州将不能出台覆盖 2015 年网络中立相关内容的法律内容、FCC 提及但还没有通过的法律内容以及可能会让 ISP 赚钱变得更困难的法律内容。FCC 表示，由于互联网访问是一项州级服务，所以他们有权推出这样的政策。在这家委员会看来，如果各级政府有了自己的网络中立相关条例那么将会给宽带网络带来更大的负担并对其传输造成障碍或不必要的负担。据悉，FCC 将在下月 14 日就网络中立废除法律提案进行投票。

4、印度国家身份识别系统 Aadhaar 数据泄漏：超 210 个中央政府网站暴露公民身份信息

HackerNews.cc11 月 21 日消息 据外媒 IBTimes 报道，印度执法部门 RTI 于近期发现超过 210 家政府网站在线曝光了该国公民身份识别系统、全球最大的生物识别系统 Aadhaar 详细信息，其中包括公民姓名、地址、Aadhaar 号码、指纹与虹膜扫描及其他敏感数据。目前尚未公布数据泄露严重程度。Aadhaar 是印度政府于 2009 年启动的一台生物识别数据库，其主要是为了收集印度超过 10 亿人口的姓名、地址、手机号以及可能更为重要的指纹、相片与虹膜扫描。Aadhaar 在这一过程中已经深入到印度公民生活的方方面面。adhaar 发行机构 UIDAI 回应：“我们对于此次事件的发生深表歉意，目前这些数据已从上述网站删除。此外，我们还将定期对其进行安全审计与更新，以及适当控制与监测内外人员、材料与数据的任何流动，以确保用户数据安全”。不过，该机构并未具体说明此次数据公布的相关细节，如有多少公民信息遭到威胁、数据在这些网站上暴露了多长时间，以及是否已有违规事件发生等。

5、阿尔及利亚电信运营商遭黑客攻击，国家电子支付系统安全引担忧

HackerNews.cc11 月 23 日消息 据外媒 11 月 21 日报道，阿尔及利亚的电信运营商 Algerie Telecom 于上周五证实，公司遭受了一系列旨在破解其系统的网络攻击事件。目前，公司已在相关部门的帮助下成功击退黑客并开启安全防御系统，以便减少企业运营损失。不过，他们尚不清楚黑客真正意图以及进一步相关细节。此外，由于网络攻击数量的迅速增加引起了阿尔及利亚政府的担忧，特别是近期所推出的电子服务项目，例如公民采用电子支付系统缴纳水电费用。信息与通信技术部部长 Iman Houda Faraoun 表示，通常由部长理事会批准的电子商务项目一旦通过，将会即日生效。不过，他们承诺将会充分保护电子商务流程，严禁外泄各金融交易数据、发票以及公民银行卡号等敏感信息。

6、优步 5700 万用户信息遭窃取 隐瞒一年不报反付黑客封口费

新浪网 11 月 23 日消息 美国网约车服务商优步 11 月 21 日承认，曾在去年 10 月遭到黑客攻击，导致全球约 5700 万名用户的个人信息被窃取。为平息事件，优步当时向黑客支付了 10 万美元，约 66 万元人民币的“封口费”。据优步透露，去年十月，两名黑客从优步使用的第三方云计算服务器上窃取了全球 5700 万名用户的姓名、邮箱地址及手机号码。这其中，60 万美国司机的姓名和驾照信息也一并暴露。为了隐瞒此事，优步当时向黑客支付了 10 万美元，使其删除这些数据。但优步同时表示，黑客并未获得用户的叫车地点记录和信用卡账号等信息。今年 8 月走马上任的优步公司 CEO 达拉·霍斯劳沙希称，自己也是刚刚得知此事。他表示，优步将从这件事中吸取教训。

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：王毓骏

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158