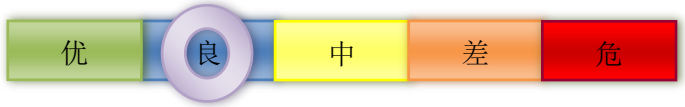
国家互联网应急中心

2017 年第 51 期

12 月 11 日-12 月 17 日

网络安全信息与动态周报

本周网络安全基本态势

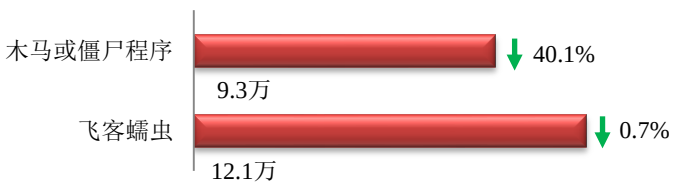


境内感染网络病毒的主机数量	•21.4万	22.8%
境内被篡改网站总数 其中政府网站数量	•2339 •44	32.8% =
境内被植入后门网站总数 其中政府网站数量	•994 •21	7.2% 5.0%
针对境内网站的仿冒页面数量	•269	20.9%
新增信息安全漏洞数量 其中高危漏洞数量	•211 •87	56.0% 44.9%

=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

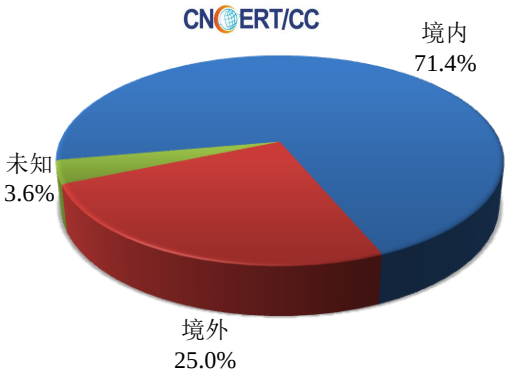
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 21.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 9.3 万以及境内感染飞客（conficker）蠕虫的主机约 12.1 万。

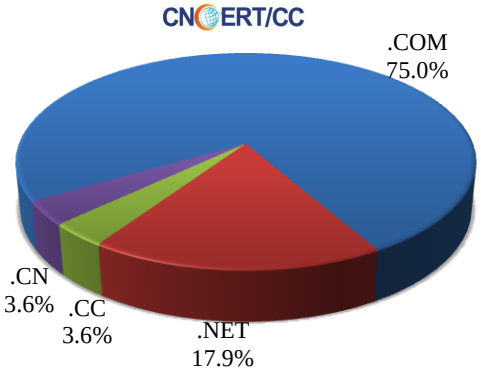


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 28 个，涉及 IP 地址 179 个。在 28 个域名中，有 25.0%为境外注册，且顶级域为.com 的约占 75.0%；在 179 个 IP 中，有约 21.8%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 1 个 IP。

本周放马站点域名注册所属境内外分布
(12/11-12/17)



本周放马站点域名所属顶级域的分布
(12/11-12/17)



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。

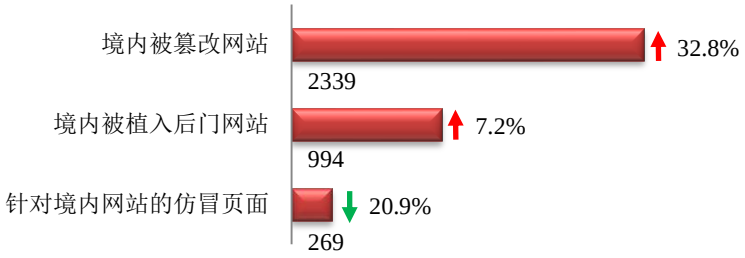
ANVA恶意地址黑名单发布地址

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。

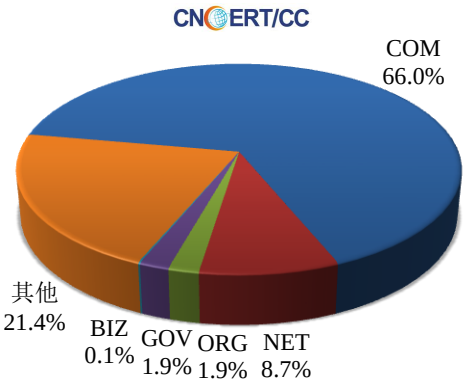
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2339 个；境内被植入后门的网站数量为 994 个；针对境内网站的仿冒页面数量为 269。

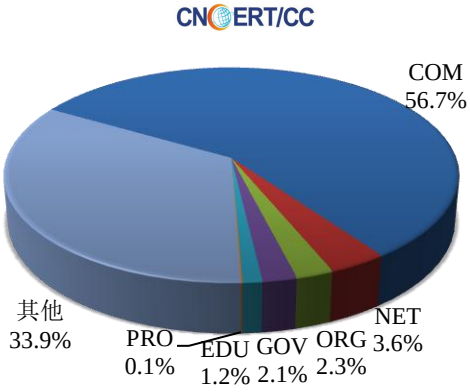


本周境内被篡改政府网站（GOV 类）数量为 44 个（约占境内 1.9%），与上周持平；境内被植入后门的政府网站（GOV 类）数量为 21 个（约占境内 2.1%），较上周环比上升了 5.0%；针对境内网站的仿冒页面涉及域名 236 个，IP 地址 130 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(12/11-12/17)

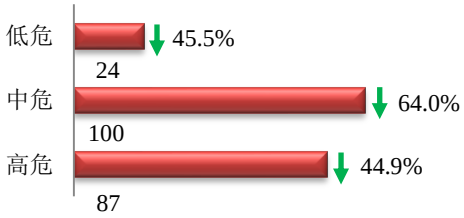


本周我国境内被植入后门网站按类型分布
(12/11-12/17)

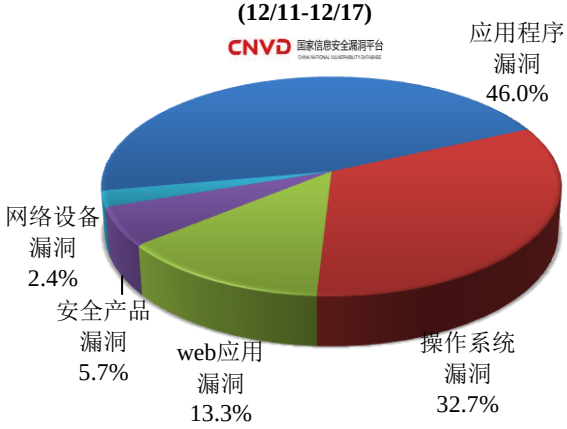


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 211 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
(12/11-12/17)



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 web 应用漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

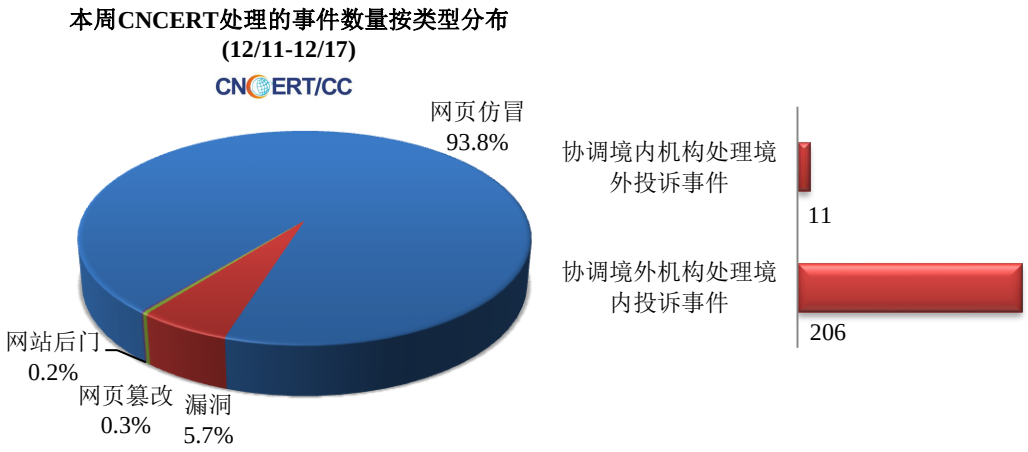
CNVD漏洞周报发布地址

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

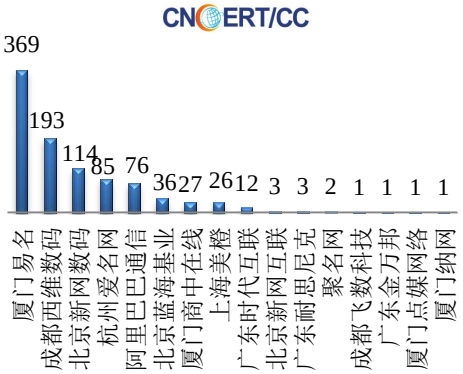
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 1241 起，其中跨境网络安全事件 217 起。



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 1164 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 1142 起和互联网服务提供商仿冒事件 8 起。

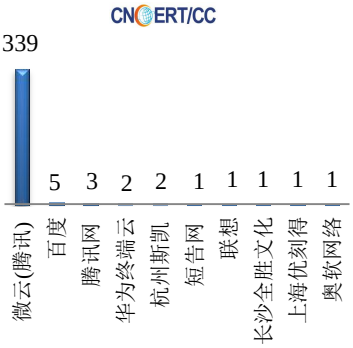
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(12/11-12/17)

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 (12/11-12/17)



本周，CNCERT 协调 10 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 356 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 (12/11-12/17)



业界新闻速递

1、北京将建设国家网络安全产业园区

新华网 12 月 12 日消息 从 12 月 12 日开幕的首届中国网络安全产业高峰论坛上获悉，工信部、北京市决定共同打造国家网络安全产业园区，并正式签署了合作协议，拉开网络安全产业创新发展的序幕。北京市经信委主任张伯旭表示，建设国家网络安全产业园区的总体目标是，将北京市建成国内领先、世界一流的网络安全高端、高新、高价值产业集聚中心。根据阶段目标，到 2020 年，将依托产业园区拉动 GDP 增长超过 3300 亿元，北京市网络安全产业力争达千亿元规模，打造不少于 3 家年收入超过 100 亿元的骨干企业。到 2035 年，依托产业园区建成我国网络安全产业“五个基地”，即国家安全战略支撑基地、国际领先的网络安全研发基地、网络安全高端产业集聚示范基地、网络安全领军人才培育基地和网络安全产业制度创新基地。目前，工信部和北京市已组建联合工作组。据了解，接下来，国家网络安全产业园区建设的重点工作将包括打造政产学研用网络安全产业生态系统，引导龙头企业建设网络安全产业“双创”平台；推动联合建设国家级和部省级实验室，建设网

络安全实训基地；设立网络安全产业园区专项基金，建立法律手段保护网络安全知识产权等。

2、美国国家标准与技术研究院（NIST）发布第二版《网络安全框架草案》

HackerNews.cc12 月 12 日消息 美国国家标准与技术研究院（NIST）发布了 NIST 网络安全框架更新的第二稿。NIST 于 2017 年 12 月 5 日发布了”改进关键基础设施网络安全框架“（也就是网络安全框架 1.1 版草案 2）提议更新的第二稿。“本第二稿草案旨在澄清，改进和加强网络安全框架，扩大其价值并使其更易用。新草案融入了收到的意见，这些意见来自 2017 年 1 月启动的公开审查流程和 2017 年 5 月的研讨会。NIST 网络安全框架于 2014 年首次发布，旨在帮助公司组织，特别是关键基础设施部门管理网络安全风险。当时，NIST 发布了“改进关键基础设施安全框架”，该文件提出了制定安全计划的网络安全标准和实践。如今，NIST 网络安全框架被认为是众多组织和企业实施的最佳实践指南。网络安全框架是根据美国前总统奥巴马发布的行政命令制定的，现在特朗普政府也认为该框架是一套由政府机构和关键基础设施运营商实施的最佳实践。特朗普现任政府发布的网络安全行政命令也要求联邦机构和关键基础设施运营商使用该框架。

3、印度于一年内两度设立 CERT——此番专门面向政府事务

E 安全 12 月 15 日消息 印度政府已经决定设立第三个计算机应急响应小组（CERT）“NIC-CERT”，旨在保护政府内的各项数字化服务。印度最早建立的 CERT 为 CERTin，使命与其它国家的 CERT 基本相同，主要负责帮助各国家机关检测并交付新兴威胁信息。印度第二个 CERT 为 Fin-CERT，专门为金融部门设立。如今印度又在全国范围内开设“NIC-CERT”，“NIC”是指国家信息中心，即印度的电子商务与电子政务组织。NIC 的职能角色意味着 NIC-CERT 将承担起保护印度政府信息基础设施的责任。NIC-CERT 目前拥有 30 名安全人员，他们将与 300 名 NIC 现任员工协同努力。这些工作人员将负责情报收集等任务，旨在发现一切可能导致印度政府遭遇攻击的蛛丝马迹，进而弄清楚如何将此类恶意活动扼杀在萌芽状态。

4、北约向网络战规则中添加“攻击性防御”条款

E 安全 12 月 11 日消息 北约成员国中的美国、英国、德国、挪威、西班牙、丹麦以及荷兰目前正考虑对国家支持型计算机黑客活动作出更为强硬的反应，将制定网络战争规则，旨在指导其部队更为广泛地部署网络攻击性武器，具体可能涉及利用网络攻击击退对方入侵行动，且计划在 2019 年年初就具体条款达成共识。相关官员认为这一理论依据可能将北约的相关实践由防御转化为反击，用以对抗俄罗斯、中国与朝鲜用于破坏西方政府职能并窃取技术的黑客手段。在北约合作网络防御卓越中心（为北约下辖之研究中心，负责协调多边规则的确立工作）工作的美国海军司令迈克尔·韦德曼表示，北约的思维模式正在发生改变，开始接受计算机与飞机及舰艇一样，拥有攻击能力。拥有 29 个成员国的北约联盟于 2014 年将网络正式认定为战场概念，同地面、空中与海洋并列，但并没有提供更具体的描述。

5、美媒：俄黑客攻击美国大批银行 从 ATM 盗走 1000 万美元

腾讯网 12 月 12 日消息 在过去两年中，美国曾经有大量的银行和零售公司遭到俄国黑客的攻击，导致数亿个用户账号被盗。据外媒最新消息，一家安全机构揭露了一个俄国黑客组织，该组织从美国等国的银行自动柜员机网络盗走了 1000 万美元。据路透社报道，日前安全研究机构 Group-iB 公开了相关的报告，称俄国黑客组

织 MoneyTaker 在过去 18 个月的时间里，针对美国和俄国的银行柜员机发动了攻击，一共盗取的金额为 1000 万美元。这个黑客组织一共攻击了 18 家银行，其中 15 家银行分布在美国，其余分布在俄国，黑客破解了银行之间的转账系统功能，并派出人员在柜员机取走了大量现金。需要指出的是，这些黑客攻击事件对于银行的消费者并无直接影响，黑客主要瞄准了银行之间的转账业务。目前有关这个 MoneyTaker 组织的更多幕后信息尚不得而知，该组织巧妙藏匿了自己的身份。在过去，他们时常更换各种攻击工具和盗取方法，绕过了银行的安全软件，另外这家黑客组织也会认真删除所有的攻击痕迹，导致银行和警方很难获得一些侦察线索。

6、暗网暴露 14 亿明文密码库，或成史上最大规模数据泄露案

HackerNews.cc12 月 14 日消息 据外媒报道，美国一家网络情报公司 4iQ 于 12 月 5 日在暗网社区论坛上发现了一个大型汇总数据库，其中包含了 14 亿明文用户名和密码组合，牵涉 LinkedIn，MySpace，Netflix 等多家国际互联网巨头。研究人员表示，这或许是迄今为止在暗网中发现的最大明文数据库集合。4iQ 研究员称他们在暗网搜寻被窃、泄露数据时从一个超过 41GB 的文件中发现了这个汇总的交互式数据库。该档案最后一次于 11 月 29 日更新，其中汇总了 252 个之前的数据泄露和凭证列表、包含 14 亿个用户名、电子邮件和密码组合、以及部分比特币和狗狗币（Dogecoin）钱包。据统计，这 14 亿数据由早期泄露的数据和凭证列表汇总而成，密码部分来自 Anti Public，Exploit.in 等凭证列表，多涉及 Anti Public、Exploit.in、LinkedIn、MySpace、Netflix、比特币、Pastebin、FM,Zoosk、YouPorn、Badoo、RedBox 等互联网公司以及类似 Minecraft 和 Runescape 这类游戏公司。

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：余江浩

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158