国家互联网应急中心

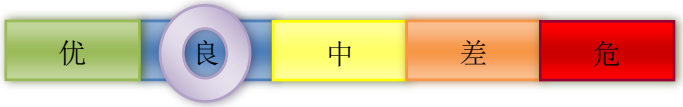
网络安全信息与动态周报

2017 年第 52 期

12 月 18 日-12 月 24 日

CNCERT/CC

本周网络安全基本态势

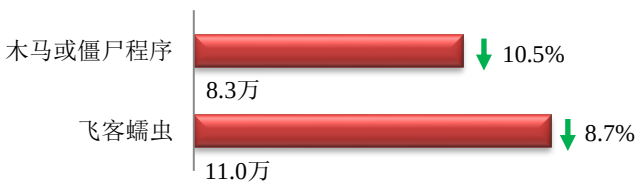


境内感染网络病毒的主机数量	• 19.3万	↓ 9.5%
境内被篡改网站总数 其中政府网站数量	• 2060 • 45	↓ 11.9% ↑ 2.3%
境内被植入后门网站总数 其中政府网站数量	• 901 • 13	↓ 9.4% ↓ 38.1%
针对境内网站的仿冒页面数量	• 353	↑ 31.2%
新增信息安全漏洞数量 其中高危漏洞数量	• 440 • 194	↑ 108.5% ↑ 123.0%

= 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

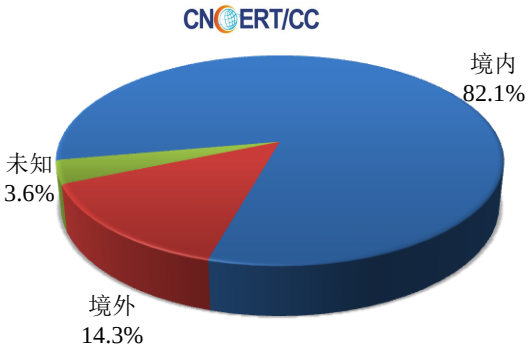
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 19.3 万个，其中包括境内被木马或被僵尸程序控制的主机约 8.3 万以及境内感染飞客（conficker）蠕虫的主机约 11.0 万。

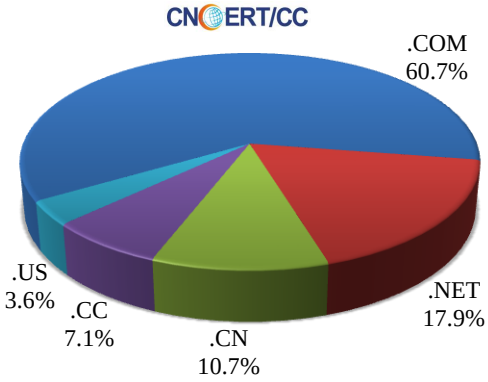


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 28 个，涉及 IP 地址 182 个。在 28 个域名中，有 14.3%为境外注册，且顶级域为.com 的约占 60.7%；在 182 个 IP 中，有约 25.8%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 1 个 IP。

本周放马站点域名注册所属境内外分布
(12/18-12/24)



本周放马站点域名所属顶级域的分布
(12/18-12/24)



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。

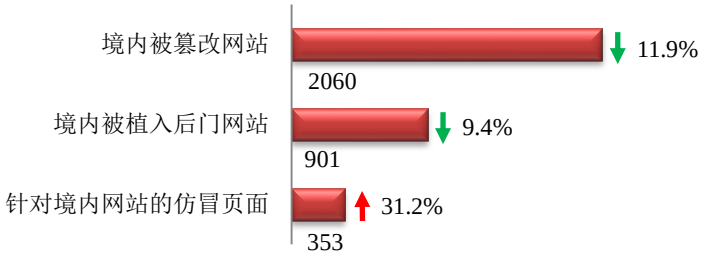
ANVA恶意地址黑名单发布地址

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。

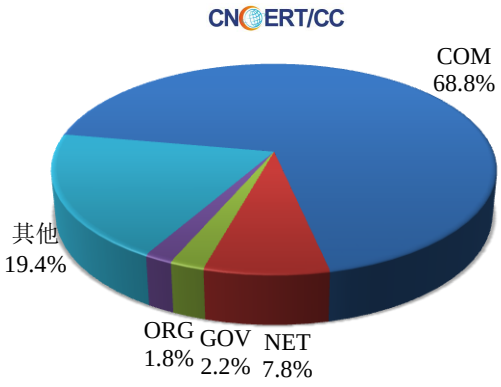
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2060 个；境内被植入后门的网站数量为 901 个；针对境内网站的仿冒页面数量为 353。

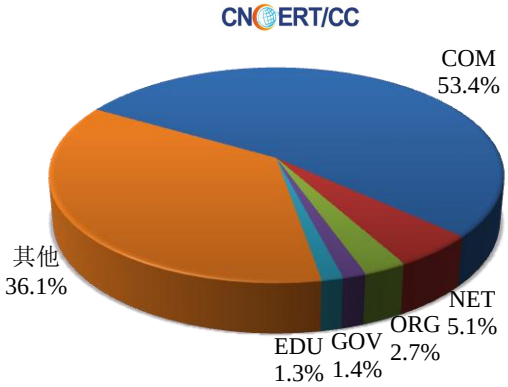


本周境内被篡改政府网站（GOV 类）数量为 45 个（约占境内 2.2%），较上周环比上升了 2.3%；境内被植入后门的政府网站（GOV 类）数量为 13 个（约占境内 1.4%），较上周环比下降了 38.1%；针对境内网站的仿冒页面涉及域名 305 个，IP 地址 143 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(12/18-12/24)

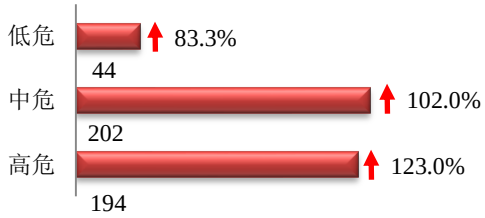


本周我国境内被植入后门网站按类型分布
(12/18-12/24)

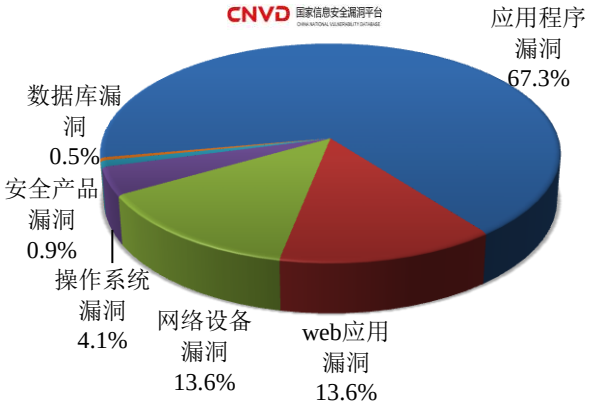


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 440 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
(12/18-12/24)



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 web 应用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。

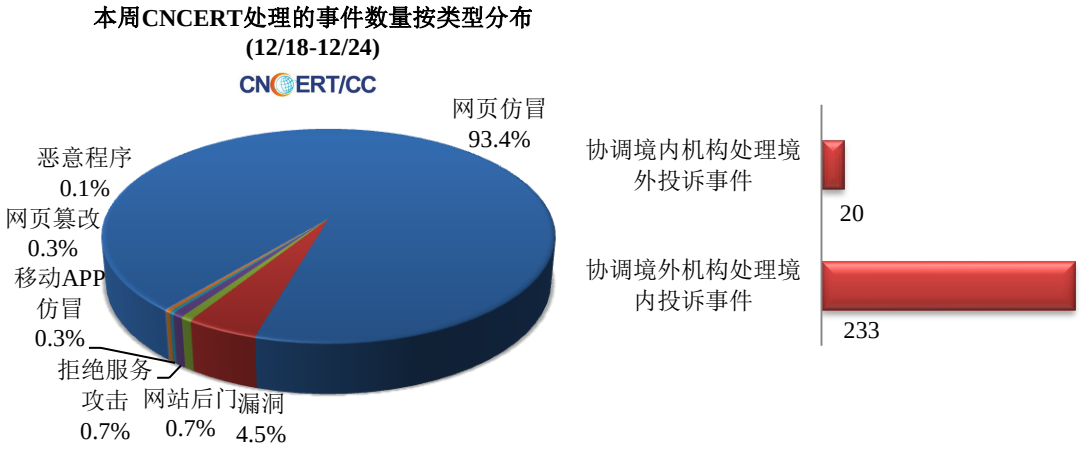
CNVD漏洞周报发布地址

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

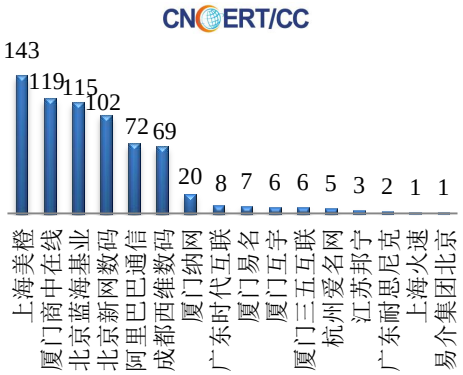
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 985 起，其中跨境网络安全事件 253 起。



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 920 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 890 起和互联网服务提供商仿冒事件 21 起。

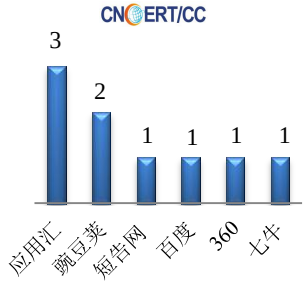
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(12/18-12/24)

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 (12/18-12/24)



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 (12/18-12/24)



业界新闻速递

1、特朗普发布首份《国家安全战略》要做三件事保护网络安全

E 安全 12 月 20 日消息 美国当地时间 2017 年 12 月 18 日下午，特朗普公布了其任职期内的首份国家安全战略报告，长达 68 页，其中强调本届政府在全球及外交政策层面将始终坚持 “美国至上”的方针，囊括了用于改善美国国家网络安全方法的行动纲要清单。白宫方面表示：美国将“投入资源以支持并提升实现网络攻击归因的能力，确保有能力作出快速反应。”网络安全战略报告总结建议指出，特朗普政府的计划将使得美国能够更轻松地“根据需求”对敌对方实施网络行动。美国政府将与美国国会合作，应对继续阻碍即时情报与信息共享、有碍网络工具规划运营以及开发的种种挑战。一旦拥有针对网络空间内恶意行为者采取行动的机会，美国将及时获悉相关风险，但在考虑应对选项时不会故意犯险。美国将努力改善美国政府已经严重老化的 IT 基础设施。美国政府还将推动一轮‘吸引、培养及挽留’各政府机构与部门网络安全专业人员队伍的努力。

2、白宫将 5G 网络部署列为国家安全首要任务

cnBeta.COM12 月 20 日消息 据外媒报道，日前，美国白宫已经将 5G 网络推出列为国家安全首要任务。该消息来自最新发布的 2017 年 12 月国家安全战略报告。在《支柱二：促进美国繁荣（Pillar II: Promote American Prosperity）》中有一个版块叫“改善美国基础设施”。白宫在这部分内容中表示，5G 网络将在全球范围内部署以此来改善美国的数字基础设施。据了解，报告部分内容将关注点放在经济上——“经济安全即国家安全”。白宫列出了一系列旨在振兴美国经济的优先行动，5G 网络部署便是其中一个。不过 5G 并不是该份报告中提及的唯一一项技术，在国土安全版块，白宫还将“反网络犯罪”也列入了优先行动，并称将使用复杂调查工具来破坏犯罪分子利用网络市场、加密货币和其他非法活动工具的能力。报告还发出呼吁，美国将需要通过把安全和经济增长放在优先位置以此来让自己在研究、技术、发明和创新领域处于领先地位。此外，报告还提到了加密、数据科学、基因编辑、先进计算、自主技术、纳米技术以及人工智能等新兴技术。

3、特朗普推翻“网络中立”规定引争议 谷歌等强烈反对

环球网 12 月 18 日消息 当地时间 12 月 15 日，美国联邦通信委员会以 3 票赞成、2 票反对的投票结果，推翻了奥巴马政府时期推出的“网络中立”规定。这一举动随即得到了共和党议员、白宫和网络服务提供商的支持，但却引起了民主党议员、互联网科技公司和消费者团体的强烈抗议。“网络中立”的规定始于 2015 年奥巴马执政期间的政策。这个政策禁止互联网的“付费优先权”，也就是禁止网络服务提供商在收取内容提供商（例如视频网站）更高的费用后，为其提供更高质量的宽带服务。通过这种手段，能确保所有合法的网络内容能以相同的速度载入，使小型互联网科技公司也能在与互联网大公司竞争时有相对公平的舞台。废除“网络中立”规定不但取消了对互联网供应商封锁网站的限制，也取消了对互联网内容提供商收费的限制，同时禁止各州采取与联邦通信委员会不同的规章政策。当地媒体报道称，反对废除“网络中立”规定的互联网公司强调，“没有了网络中立性规定，网络运营商将占据互联网的主导权，阻碍互联网领域的创新和机遇，甚至危害到美国的互联网的自由。他们强调，不应把互联网的决定权交给运营商，不能让运营商影响左右网民的互联网使用选择，危害到公开开放的互联网。”

4、日本拟设太空及网络部队 未来或向他国发动网络攻击

新浪网 12 月 18 日消息 据共同社 12 月 18 日报道，日本政府相关人士 17 日透露，政府已基本决定，在防卫省自卫队内新设统管太空及网络空间、电子战负责部队的拥有司令部功能的上级部队，并写入明年下半年修改的防卫力建设方针《防卫计划大纲》（防卫大纲）。预计此事将在近期召开的国家安全保障会议（NSC）四大臣会议上获得批准。太空和网络被定位为继陆海空后的第 4 和第 5“战场”，但与已拥有具司令部功能的专门组织的其他国家军队相比，日本已然落后。此举旨在加强应对安全保障方面的新课题。三个自卫队均有统管现场部队的上级部队，海自有自卫舰队，空自有航空总队，陆自有陆上总队（计划明年 3 月新设）。据相关人士透露，本次新设的部队与上述部队级别相同，将整合太空、网络、电子战的各专业部队。司令将由将官级别担任，正式名称尚未确定。

5、数据分析公司 Alteryx 因 AWS S3 配置不当，致 1.23 亿美国家庭敏感信息在线泄露

HackerNews.cc12 月 21 日消息 据外媒报道，加利福尼亚网络安全公司 UpGuard 表示，包含数据分析公司 Alteryx 敏感信息的亚马逊网络服务（AWS）S3 云存储器因配置不当，导致逾（36GB）1.23 亿美国家庭的详细信息在线泄露，其中几乎蕴含每个美国家庭的种族和名族信息。虽然这些数据的电子表格使用了匿名标识符，但其他几十亿字段中的信息却非常详细，比如家庭住址、联系信息、抵押贷款状况、财务状况以及非常具体的购买行为分析。根据 UpGuard 的说法，其网络风险团队曾于今年 10 月发现 Alteryx 托管的 S3 云存储桶存在信息泄漏迹象，该存储桶中还包含数据分析公司 Alteryx 的合作伙伴、消费者信用报告机构 Experian 和美国人口普查局的数据集。而这些完整的 Experian 的 ConsumerView 营销数据库和 2010 年美国人口普查的全部数据集都是可用的。目前，Alteryx 已展开调查并表示，虽然此次泄露的文件包含了第三方内容供应商营销数据，但他们承诺，泄露的云数据库现已在互联网上封锁，文件中的信息不会对任何消费者造成身份盗用的风险。

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：刘栋

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158