国家互联网应急中心

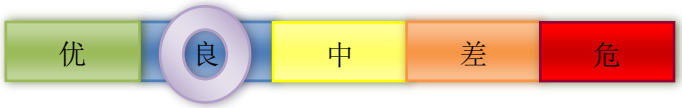
网络安全信息与动态周报

2018 年第 1 期

1 月 1 日-1 月 7 日

CNCERT/CC

本周网络安全基本态势

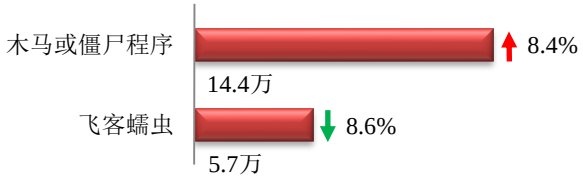


境内感染网络病毒的主机数量	•20.1万	↑ 3.0%
境内被篡改网站总数 其中政府网站数量	•2210 •44	↓ 7.2% ↑ 4.8%
境内被植入后门网站总数 其中政府网站数量	•827 •38	↓ 3.6% ↑ 46.2%
针对境内网站的仿冒页面数量	•407	↑ 9.4%
新增信息安全漏洞数量 其中高危漏洞数量	•219 •63	↓ 25.5% ↓ 30.8%

═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

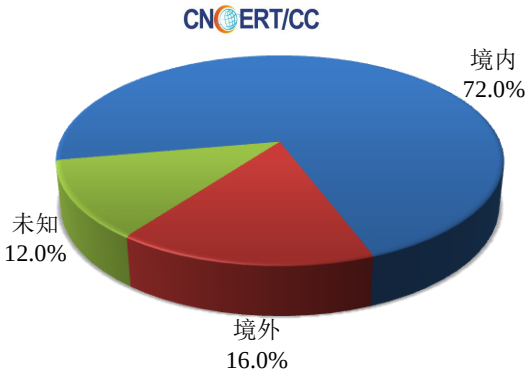
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 20.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 14.4 万以及境内感染飞客（conficker）蠕虫的主机约 5.7 万。

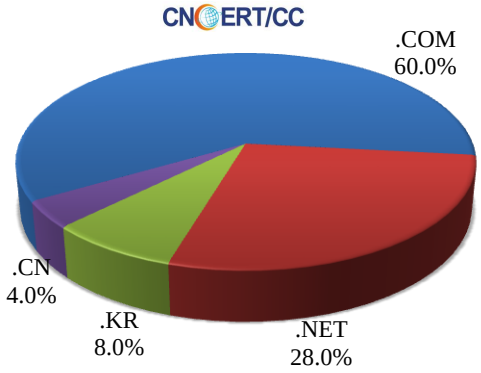


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 25 个，涉及 IP 地址 181 个。在 25 个域名中，有 16.0%为境外注册，且顶级域为.com 的约占 60.0%；在 181 个 IP 中，有约 28.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 1 个 IP。

本周放马站点域名注册所属境内外分布
(1/1-1/7)



本周放马站点域名所属顶级域的分布
(1/1-1/7)



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。

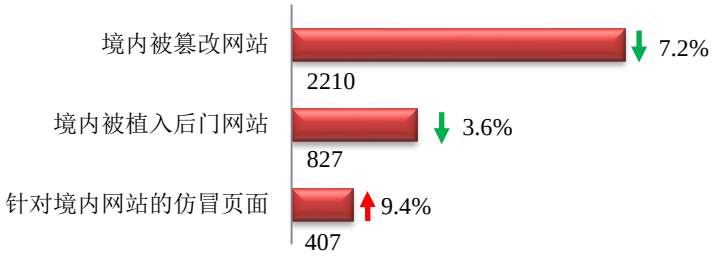
ANVA恶意地址黑名单发布地址

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。

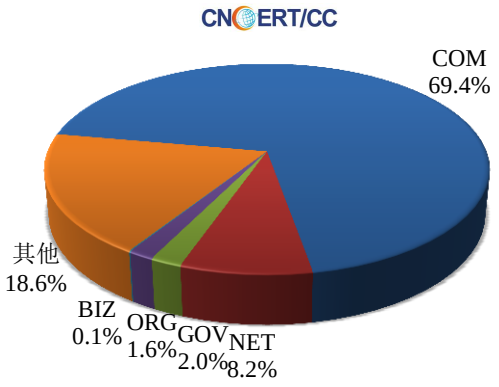
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2210 个；境内被植入后门的网站数量为 827 个；针对境内网站的仿冒页面数量为 407。

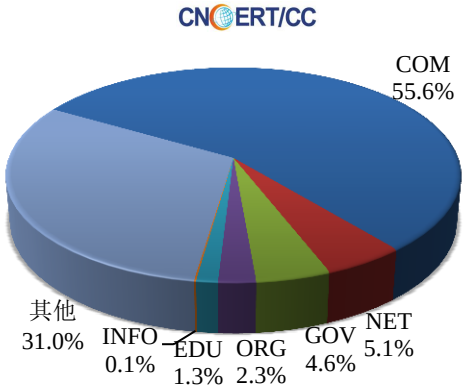


本周境内被篡改政府网站（GOV 类）数量为 44 个（约占境内 2.0%），较上周环比上升了 4.8%；境内被植入后门的政府网站（GOV 类）数量为 38 个（约占境内 4.6%），较上周环比上升了 46.2%；针对境内网站的仿冒页面涉及域名 330 个，IP 地址 176 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(1/1-1/7)

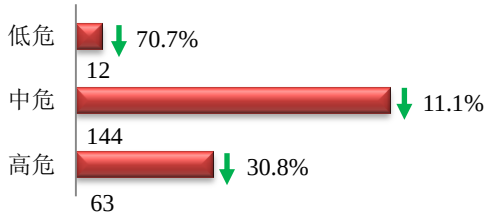


本周我国境内被植入后门网站按类型分布
(1/1-1/7)

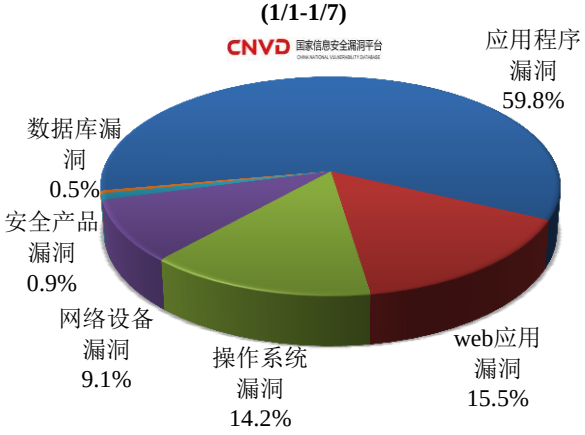


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 219 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
(1/1-1/7)



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 应用漏洞和操作系统漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

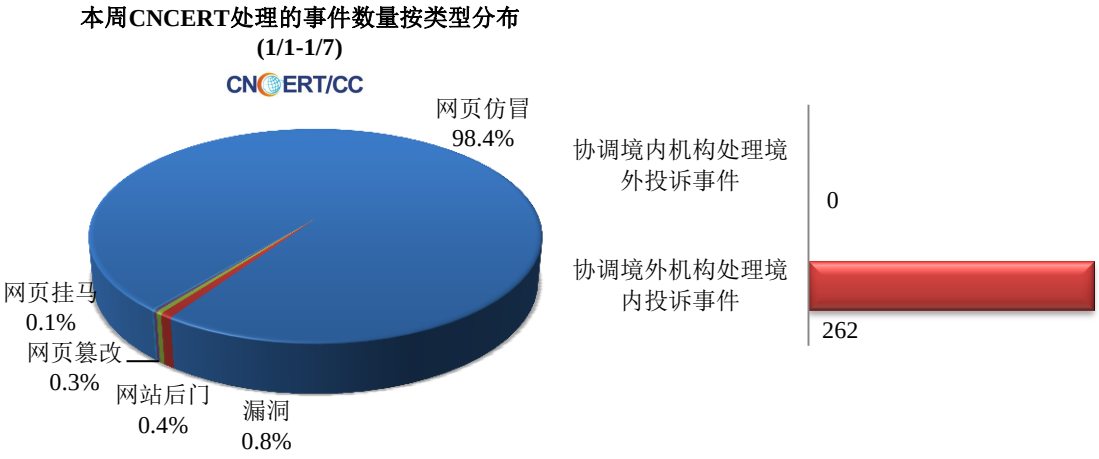
CNVD漏洞周报发布地址

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。

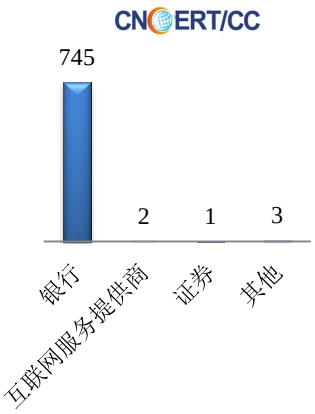
本周事件处理情况

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 763 起，其中跨境网络安全事件 262 起。

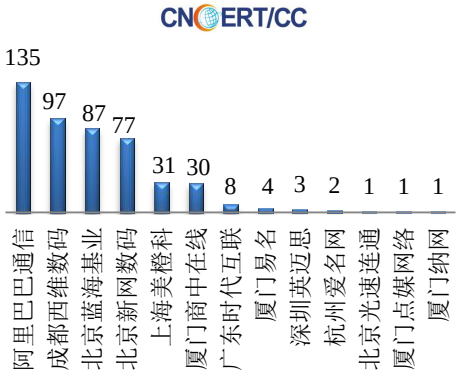


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 751 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 745 起和互联网服务提供商仿冒事件 2 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(1/1-1/7)

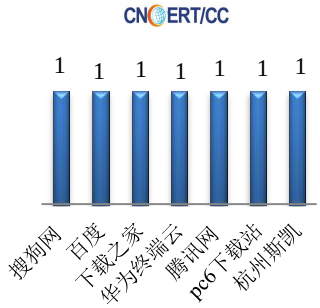


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (1/1-1/7)



本周，CNCERT 协调 7 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 7 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 (1/1-1/7)



业界新闻速递

1、工信部加强工业互联网安全保障工作

中国政府网 1 月 4 日消息 为加快我国工业控制系统信息安全保障体系建设，提升工业企业工业控制系统信息安全防护能力，促进工业信息安全产业发展，工业和信息化部日前印发《工业控制系统信息安全行动计划（2018—2020 年）》。工信部信息化和软件服务业司相关负责人今日表示，这是为工业互联网安全保障工作制定了时间表和路线图，进一步明确了部门、地方和企业做什么和怎么做，为下一步开展工控安全工作提供了依据和指导。《行动计划》实施的主要目标包括，到 2020 年，建成工控安全管理工作体系，全系统、全行业工控安全意识普遍增强，建成“一网一库三平台”。同时，促进工业信息安全产业发展，提升产业供给能力，培育一批龙头骨干企业，创建 3 个至 5 个国家新型工业化产业化产业示范基地。对于“一网一库三平台”，上述负责人解释说，“一网”是指全国工控安全在线监测网络，“一库”是指工控安全应急资源库，“三平台”是指工控安全仿真测试平台、信息共享平台和信息通报平台。

2、日本政府拟 2020 年新设网络太空组织

E 安全 1 月 6 日消息 日本政府计划 2020 年设立一个由防卫大臣直接管理的新组织，希望以此提升在网络空间和太空的防卫能力。日本正讨论是否将该计划写入新的《防卫计划大纲》（计划于 2018 年底重新审定）。据报道，新组织将由一名将官担任领导，并从日本自卫队海、陆、空三军抽调人员，其地位将与日本陆上总队（计划于 2018 年 3 月设立）、日本航空总队和日本自卫舰队持平。新组织的管理权限集中在网络与太空领域。新组织将包含现有的网络防卫队，并新设太空部队。该网络防卫队将负责监控日本防卫省和自卫队的网络，日本政府计划 2019 财年为其增配人员，由现在的 110 人扩充至 150 人。日本预计将于本世纪 20 年代初期组建太空部队，太空部队将监控可能会阻碍卫星运转的太空垃圾和卫星武器。太空和网络空间被定位为继海陆空之后的第四和第五战场。日本方面担心，如果网络遭受攻击，日本防卫省和自卫队的指挥通信系统以及民众的生活将会受到广泛影响。与美国、中国和俄罗斯等国的武装部队相比，日本自卫队在网络及太空领域已远远落后。

3、印尼正式成立负责网络安全的政府机构

人民网 1 月 4 日消息 1 月 3 日，根据 2017 年 5 月 19 日佐科总统签署的 2017 年第 53 号总统令，印尼政府宣布成立新的“国家网络安全局”（the National Cyber and Encryption Agency，简称 BSSN），以对付网上的宗教极端主义和假新闻。印尼总统佐科当天在总统府宣布，委任国家保密局前局长佐科·塞蒂亚迪（Djoko Setiadi）来领导新成立的“国家网络安全局”。该局的工作范围包括取缔恐怖分子网络、对付网上仇恨言论等。根据 2017 年 12 月 16 日佐科签署的 2017 年第 133 号总统令，新成立的“国家网络安全局”直接在总统领导之下，对总统负责。之前的类似机构是 1946 年成立的“国家保密局”（the National Encryption Agency），一直在政法安全事务统筹部部长的领导之下。新的规则强化了“国家网络安全局”的地位与功能，该局属于非内阁政府机构，但该局局长拥有政府部长级别。处理网络安全工作的协调涉及到国家网络安全局、印尼国防部（TNI）、国家情报局（BIN）、国家反恐局（BNPT）及政法安全事务统筹部所属的国家禁毒局（BNN）。

4、美国土安全部超过 24 万员工的个人数据被泄

E 安全 1 月 5 日消息 美国国土安全部（DHS）于美国当地时间 2018 年 1 月 3 日发表声明称，其下属监察长办公室（OIG）2014 年遭遇一起数据泄露事件，其案件管理系统逾 24.7 万 DHS 员工和未知数量的其它相关人员的个人信息受到影响。这起事故并非因外部黑客入侵所致，而是前雇员未经授权擅自转移 OIG 案件管理系统的数据，DHS 称个人信息不是这起数据转移的主要目标。美媒 2017 年 11 月曾报道了美国国土安全部（DHS）这起事件，当时并未得到 DHS 的证实。DHS 表示，OIG 调查案件管理系统共包含 24.7167 万名 DHS 员工的个人信息，此外还包括 2002 年至 2014 年 OIG 案件涉及的调查对象、证人以及原告等信息。DHS 并未提及受影响的非雇员数量。DHS 并未在这份声明中提及受影响的具体个人信息。据美媒推测，这些个人信息可能包含普通信息和高度敏感信息，比如姓名、电话号码、社保号和财务数据。DHS 表示正在采取安全预防措施，以限制他人获取这些信息。

5、英特尔芯片被曝两个漏洞：1995 年之后系统都受影响

新浪网 1 月 4 日消息 北京时间 1 月 4 日上午消息，安全研究人员在英特尔芯片中发现两个关键漏洞，利用

漏洞，攻击者可以从 App 运行内存中窃取数据，比如密码管理器、浏览器、电子邮件、照片和文档中的数据。研究人员将两个漏洞叫作“Meltdown”和“Spectre”，他们还说，1995 年之后的每一个系统几乎都会受到漏洞的影响，包括计算机和手机。研究人员在英特尔芯片上验证了自己的发现，这些芯片最早可以追溯到 2011 年，随后研究人员公布了概念验证代码，让用户在机器上测试。发现 Meltdown 漏洞的安全研究人员丹尼尔·格鲁斯（Daniel Gruss）在邮件中表示：“攻击者也许有能力窃取系统中的任何数据。”研究报告则说：“利用 Meltdown 漏洞，攻击者不只可以进入核心内存，还可以读取目标机器的所有物理内存数据。”Windows、Macs 和 Linux 系统无一幸免，都受到漏洞的威胁。有许多云服务使用英特尔服务器，它们也会受到影响，正因如此，亚马逊、微软、谷歌已经行动起来，给云服务打补丁，按计划中断服务，防止攻击者窃取数据，攻击者可能会在相同的共享云服务器上窃取其它数据。

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：丁丽

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158