国家互联网应急中心

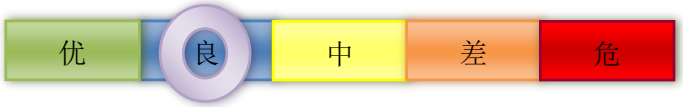
# 网络安全信息与动态周报

**2018 年第 8 期**

**2 月 19 日-2 月 25 日**

CNCERT/CC

## 本周网络安全基本态势

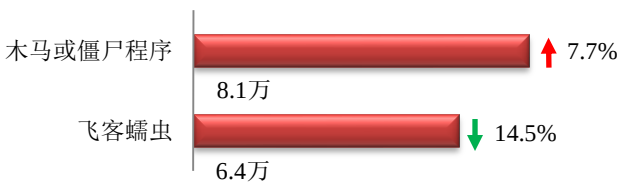



| | | |
|---|---|---|
| 境内感染网络病毒的主机数量 | •14.5万 | 3.3% |
| 境内被篡改网站总数<br>其中政府网站数量 | •1793<br>•29 | 8.4%<br>14.7% |
| 境内被植入后门网站总数<br>其中政府网站数量 | •645<br>•4 | 59.3%<br>20.0% |
| 针对境内网站的仿冒页面数量 | •92 | 100.0% |
| 新增信息安全漏洞数量<br>其中高危漏洞数量 | •146<br>•31 | |

*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*

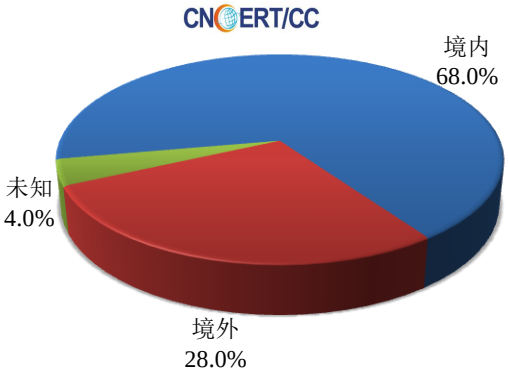
## 本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 14.5 万个，其中包括境内被木马或被僵尸程序控制的主机约 8.1 万以及境内感染飞客（conficker）蠕虫的主机约 6.4 万。

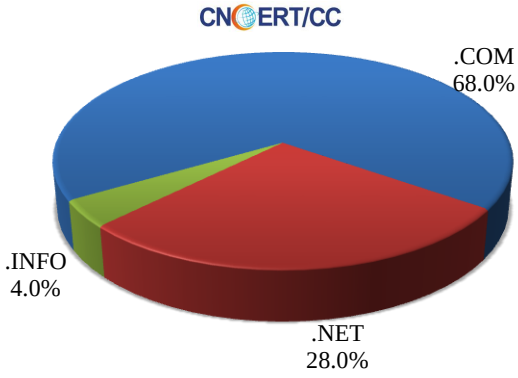


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 25 个，涉及 IP 地址 50 个。在 25 个域名中，有 28.0%为境外注册，且顶级域为.com 的约占 68.0%；在 50 个 IP 中，有约 36.0%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 1 个 IP。

**本周放马站点域名注册所属境内外分布**
**(2/19-2/25)**




**本周放马站点域名所属顶级域的分布**
**(2/19-2/25)**




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。

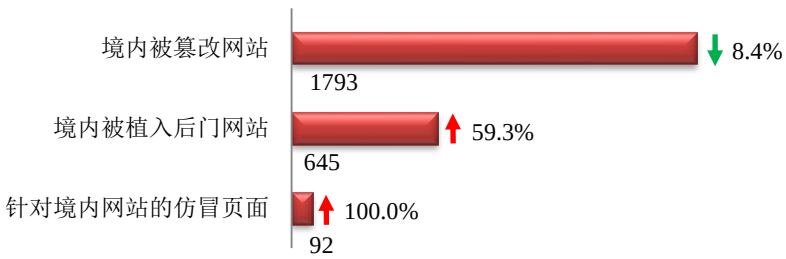
**ANVA恶意地址黑名单发布地址**

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。*

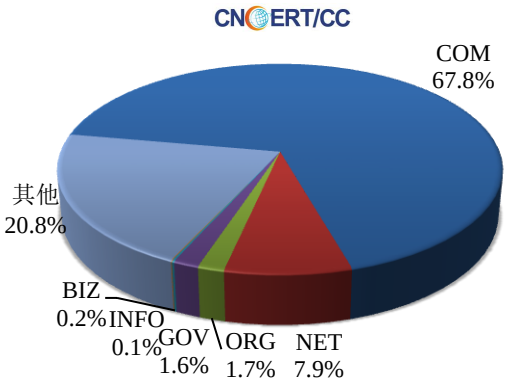
## 本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1793 个；境内被植入后门的网站数量为 645 个；针对境内网站的仿冒页面数量为 92。

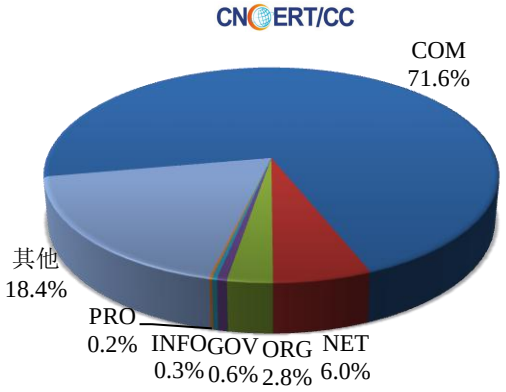


本周境内被篡改政府网站（GOV 类）数量为 29 个（约占境内 1.6%），较上周环比下降了 14.7%；境内被植入后门的政府网站（GOV 类）数量为 4 个（约占境内 0.6%），较上周环比下降了 20.0%；针对境内网站的仿冒页面涉及域名 80 个，IP 地址 39 个，平均每个 IP 地址承载了约 2 个仿冒页面。

**本周我国境内被篡改网站按类型分布**
**(2/19-2/25)**

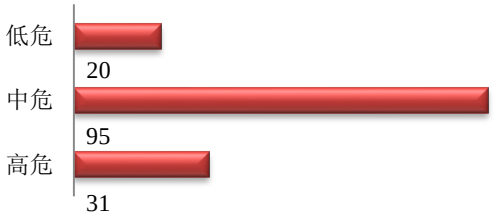



**本周我国境内被植入后门网站按类型分布**
**(2/19-2/25)**

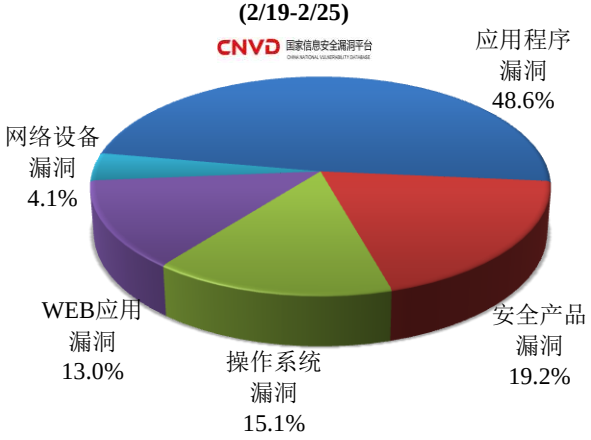



## 本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 146 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**
**(2/19-2/25)**




本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是安全产品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**

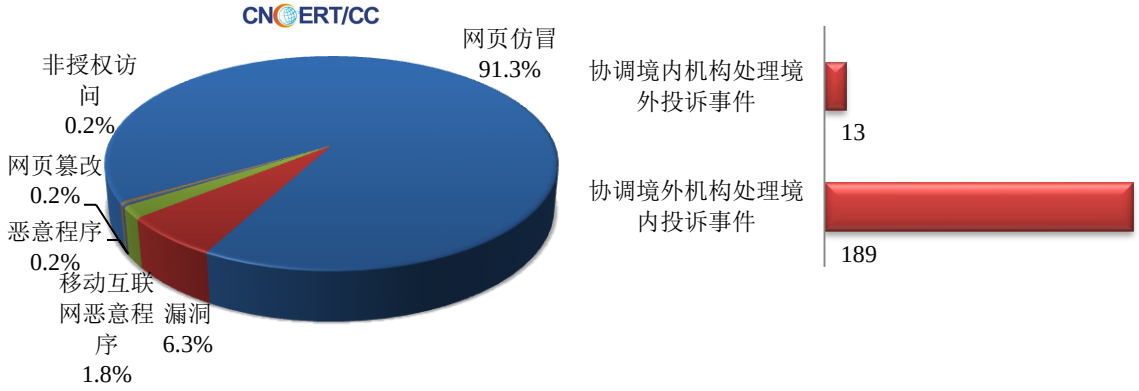
http://www.cnvd.org.cn/webinfo/list?type=4

*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

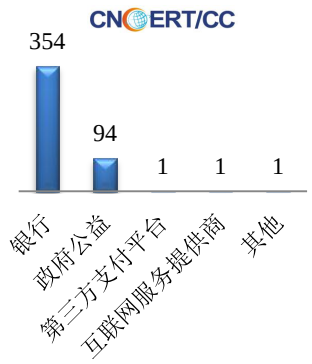
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 494 起，其中跨境网络安全事件 202 起。

**本周CNCERT处理的事件数量按类型分布 (2/19-2/25)**

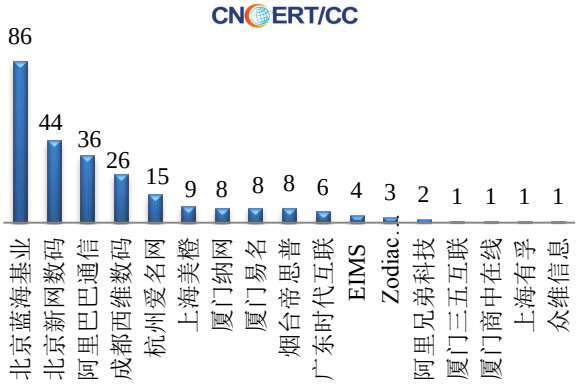



本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 451 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 354 起和政府公益仿冒事件 94 起。

**本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(2/19-2/25)**




**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 (2/19-2/25)**



## 业界新闻速递

### 1、美联邦公报公布 FCC 新规 网络中立废除倒计时开始

cnBeta.COM2 月 23 日消息 美国联邦通讯委员会（FCC）在去年十二月投票废除了 2015 年奥巴马政府确立的网络中立原则（网络中立和电信法案第二章），尽管有许多国会议员和企业与民众的阻挠，新的剥除网络中立互联网监管新政正式生效的倒计时已经开始。本周四，美国政府通过《联邦公报》（FederalRegister）正式发布剥除网络中立的新规“恢复网络自由”，这为挑战规则变化的反对者提供了 60 天的倒计时，新法规公布后，反对者可对其发起诉讼，4 月 23 日是新规正式生效日，也是挑战规则变化者的最后截止日。“网络中立”特指平等地对待互联网上的流量，2015 年的时候，美前总统巴拉克·奥巴马签署了由民主党推动的这项规则。“网络中立”准则禁止互联网服务提供商（ISP）放慢或阻止某些网站 / 服务的访问，也不允许 ISP 向客户收取“更快的互联网访问费用”。支持者们表示该规则可确保宽带企业不会滥用手上的权力，Facebook、Google、Twitter 等企业亦发声拥护。

### 2、美国司法部网络安全工作组将重点关注美国大选操纵情况

cnBeta.COM2 月 22 日消息 据外媒 SlashGear 报道，美国司法部将成立一个名为“网络数字工作组”的全新网络安全工作组。这一新的安全举措将由美国司法部长杰夫·塞申斯（Jeff Sessions）命令创建，他曾表示恐怖分子和其他人曾处于恶意原因利用互联网。网络数字工作组将评估解决这些问题的方法。根据塞 Sessions 的说法，特别工作组主要关心的是通过在线研究美国选举，避免再次发生 2016 年的情况。除了研究与在线平台相关的选举干涉之外，网络数字工作组还将优先考虑与网络安全相关的关键基础设施干扰，互联网被用来传播危险意识形态和招募新成员的方式，以及技术如何被用来“避免或阻碍执法”，黑客如何窃取大量数据及劫持计算机。司法部警告说，新的工作组不仅限于这些任务，而是它将关注其后可能涉及的其他事情。这个工作组的第一份报告将在六月底之前提交给美国司法部长。

### 3、SEC 发布新指导规则，上市公司必须披露更多有关网络安全风险的信息

腾讯网 2 月 23 日消息 近日，美国证券交易委员会（即 U.S. Securities and Exchange Commission，以下简称 SEC）正式颁布了全新指导规则，要求各家上市公司在披露有关网络安全风险问题时向社会大众公布更多具体信息，并且要在这个问题上更加具有先见性，尽最大努力在攻击事件或泄露事件发生之前准确预料到相关情景。此次声明在 2011 年颁布的指导原则的基础之上进行了进一步拓展，与此同时也针对相关人士给出了警告，命令他们不得在提前知晓某些尚未公开的网络安全问题的情况下进行股票交易。SEC 在全新指导原则中明确规定，各家公司务必要在最大程度上制定相关政策以便快速评估网络安全风险以及向大众公布这些风险的合适时机。不仅如此，SEC 还规定公司高层管理人员、董事会成员和其他公司内部人士在掌握公众尚未知晓的网络安全风险的情况下不得进行股票交易。

### 4、白帽黑客“攻击”新加坡国防部网络 三周抓 35 漏洞

环球网 2 月 22 日消息 新加坡国防部去年底宣布推出漏洞悬赏计划，雇用漏白帽黑客“攻击”新加坡国防部八个连接互联网的重要系统。据新加坡《联合早报》2 月 21 日消息，200 多名海内外高手“入侵”新加坡国防部属下的网络系统，三个星期里抓到 35 个漏洞，共获得约两万美元奖金。据报道，漏洞悬赏计划（Bug Bounty Programme）是雇用白帽黑客“攻击”国防部八个连接互联网的重要系统， 包括国防部网站、国民服役网站及使用 I-net 系统让国防部和新加坡武装部队人员上网的电邮服务。共有 264 名白帽黑客在今年 1 月 15 日至 2 月 4 日间参与这项计划，其中 100 名来自本地的白帽黑客社群。白帽黑客指的是那些利用自身黑客技术，来测试网络及系统韧性的一群善意黑客。在为期三个星期的活动中，这些白帽黑客抓到 35 个漏洞，新加坡国防部共发出 1 万 4750 美元的奖金。每个漏洞的奖金额介于 250 美元至 2000 美元，取决于寻获漏洞的复杂程度和关键性。

## 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。截至 2017 年，CNCERT 与 72 个国家和地区的 211 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：姚力

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158