国家互联网应急中心

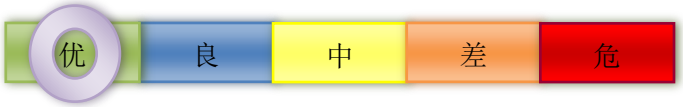
网络安全信息与动态周报

2018 年第 6 期

2 月 5 日-2 月 11 日

CNCERT/CC

本周网络安全基本态势

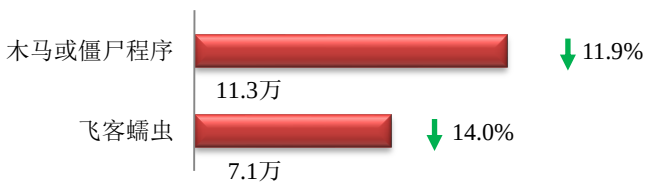


境内感染网络病毒的主机数量	• 18.4万	↓ 12.7%
境内被篡改网站总数 其中政府网站数量	• 1865 • 28	↓ 6.4% ↓ 6.7%
境内被植入后门网站总数 其中政府网站数量	• 717 • 9	↓ 8.7% ↓ 35.7%
针对境内网站的仿冒页面数量	• 187	↓ 41.2%
新增信息安全漏洞数量 其中高危漏洞数量	• 284 • 114	↓ 25.7% ↑ 12.9%

= 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

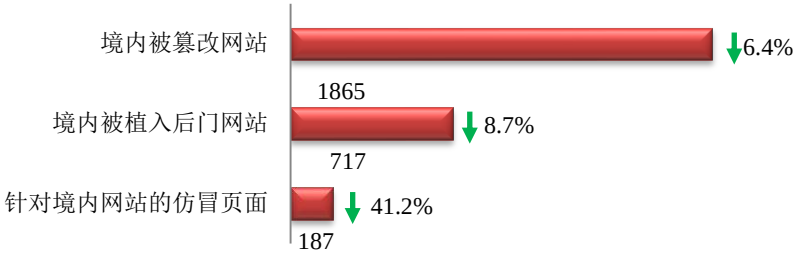
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 18.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 11.3 万以及境内感染飞客（conficker）蠕虫的主机约 7.1 万。



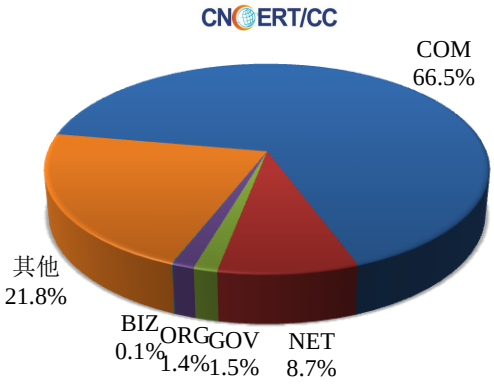
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1865 个；境内被植入后门的网站数量为 717 个；针对境内网站的仿冒页面数量为 187。

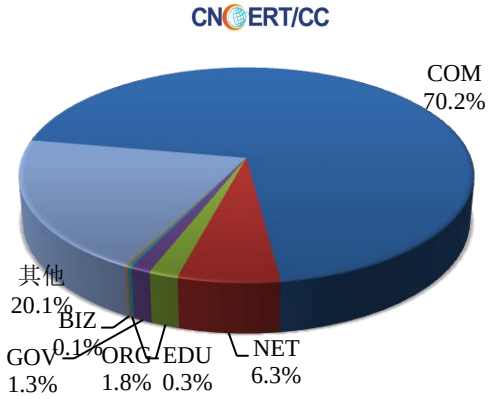


本周境内被篡改政府网站（GOV 类）数量为 28 个（约占境内 1.5%）；境内被植入后门的政府网站（GOV 类）数量为 9 个（约占境内 1.3%），较上周环比下降了 35.7%；针对境内网站的仿冒页面涉及域名 157 个，IP 地址 60 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(2/5-2/11)

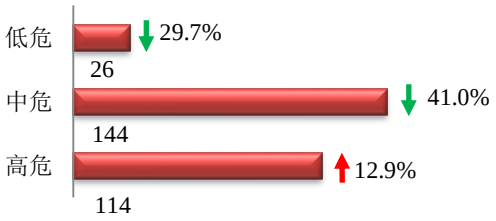


本周我国境内被植入后门网站按类型分布
(2/5-2/11)

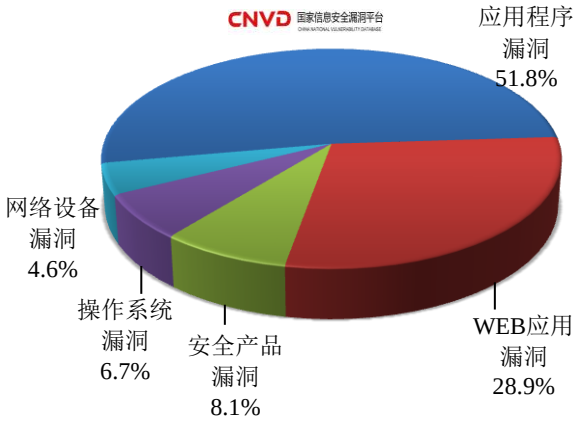


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 284 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
(2/5-2/11)



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 应用漏洞和安全产品漏洞。

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

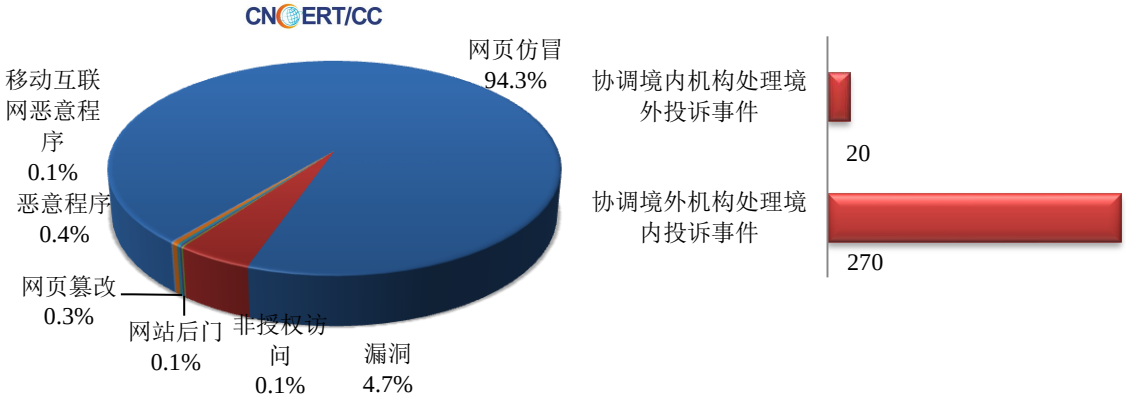
http://www.cnvd.org.cn/webinfo/list?type=4

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

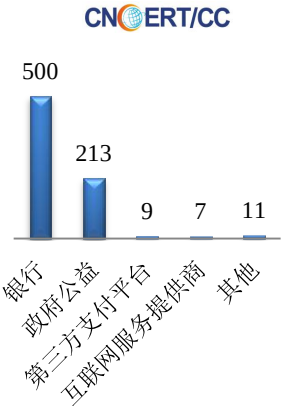
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 785 起，其中跨境网络安全事件 290 起。

本周CNCERT处理的事件数量按类型分布
(2/5-2/11)

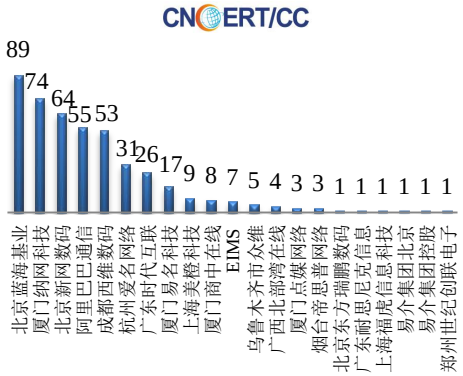


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 740 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 500 起和政府公益仿冒事件 213 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(2/5-2/11)

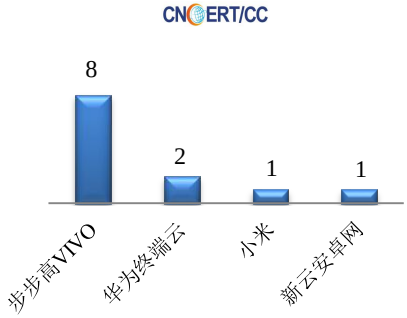


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (2/5-2/11)



本周，CNCERT 协调 4 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 12 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 (2/5-2/11)



业界新闻速递

1、平昌冬奥会开幕式期间服务器遭黑客入侵

据韩国媒体报道，平昌冬奥会组委会 2 月 10 日称，在前一天的平昌冬奥会开幕式期间，其服务器遭到身份不明的黑客入侵，导致主媒体中心的 IPTV 发生故障。为防止进一步损害，平昌冬奥会组委会关闭了服务器，但导致其官方网站不能正常运作，观众无法打印冬奥会的门票。直至今晨 8 时，冬奥会网站才恢复正常。但目前，黑客身份和从哪里发动的入侵还不得而知。此前，网络安全专家曾警告称，平昌冬奥会将成为黑客的重点袭击目标。

2、美国阻止中国投资科技行业法案遭企业反对或将缓和

2 月 9 日早间消息，据路透社援引知情人士消息称，在多家美国大公司因为担心营收降低而提出抗议后，美国国会的一项旨在阻止中国购买敏感技术的立法提案在态度上有所缓和。参众两院的这两份提案希望扩大美国外商投资委员会（CFIUS）的权力，阻止中国收购美国的复杂技术。这份两党提案也获得了特朗普政府的支持。

3、欧洲刑警组织联合英国国家犯罪调查局取缔 Luminosity RAT 幕后团伙

2 月 6 日报道，隶属欧洲刑警组织的欧洲网络犯罪中心和英国犯罪调查局于近期披露了一项国际执法行动的细节 — 来自欧洲、美国和澳大利亚的十几家执法机构联合拆除了一个 与 “ Luminosity RAT ” 远程访问木马（又名 LuminosityLink）有关的犯罪团伙。 据悉，Luminosity RAT 可以禁用目标设备上的防病毒和反恶意软件，执行诸如记录击键、窃取数据和密码、开启网络摄像头监视用户等命令。

4、美国参议员议案：美国政府应封杀华为和中兴网络设备

2 月 8 日早间消息，美国两名共和党参议员周三提出一项议案，希望禁止美国政府购买或租用来自华为或中兴的电信设备。“ 华为相当于中国政府的一个部门，他们完全有能力通过黑入自家设备来窃取美国官员的信息。” 阿肯色州参议员汤姆·考顿（Tom Cotton）说，“ 还有很多公司能满足我们的技术需求，我们不能让给让中国这么容易窃听我们。”

5、美国酝酿虚拟货币监管路线图 市场行情跌势未止

2 月 6 日，美国参议院银行、住房及城市事务委员会将举行一场有关虚拟货币的听证会。美国媒体认为，这场名为 “ 虚拟货币：美国证监会（SEC）和商品期货交易委员会（CFTC）的监督作用 ” 的听证会，将成为虚拟货币面临的一个关键时刻。

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：温森浩

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158