国家互联网应急中心

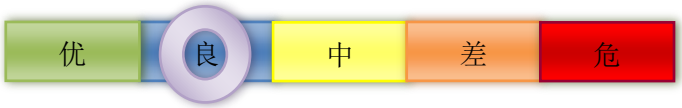
网络安全信息与动态周报

2018 年第 3 期

1 月 15 日-1 月 21 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	•23.9万	↑ 18.5%
境内被篡改网站总数 其中政府网站数量	•2435 •42	↑ 15.0% ↓ 4.5%
境内被植入后门网站总数 其中政府网站数量	•908 •37	↑ 17.5% ↑ 15.6%
针对境内网站的仿冒页面数量	•333	↓ 20.5%
新增信息安全漏洞数量 其中高危漏洞数量	•410 •128	↑ 59.5% ↑ 17.4%

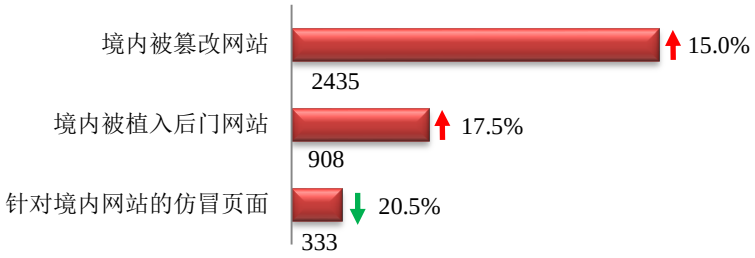
═表示数量与上周相同　↑表示数量较上周环比增加　↓表示数量较上周环比减少

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 23.9 万个，其中包括境内被木马或被僵尸程序控制的主机约 14.2 万以及境内感染飞客（conficker）蠕虫的主机约 9.7 万。

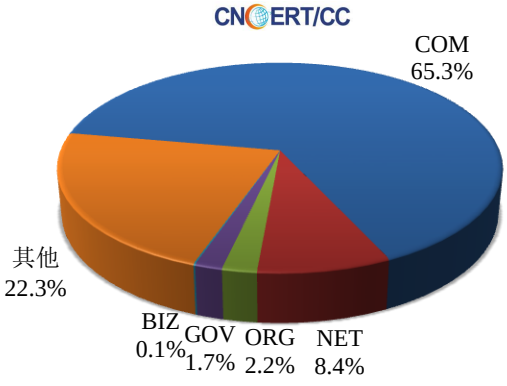
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2435 个；境内被植入后门的网站数量为 908 个；针对境内网站的仿冒页面数量为 333。

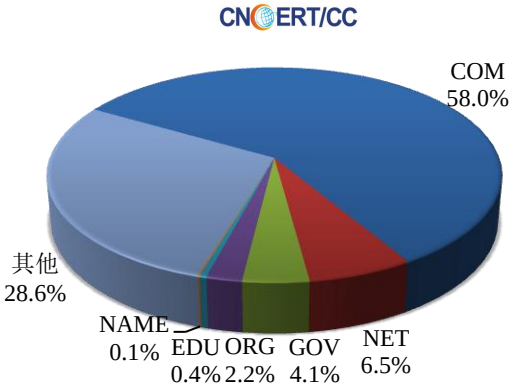


本周境内被篡改政府网站（GOV 类）数量为 42 个（约占境内 1.7%），较上周环比下降了 4.5%；境内被植入后门的政府网站（GOV 类）数量为 37 个（约占境内 4.1%），较上周环比上升了 15.6%；针对境内网站的仿冒页面涉及域名 276 个，IP 地址 141 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(1/15-1/21)

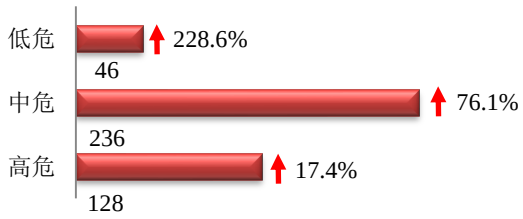


本周我国境内被植入后门网站按类型分布
(1/15-1/21)

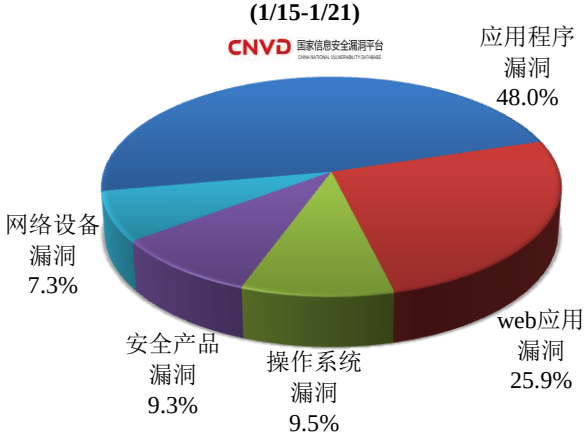


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 410 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
(1/15-1/21)



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

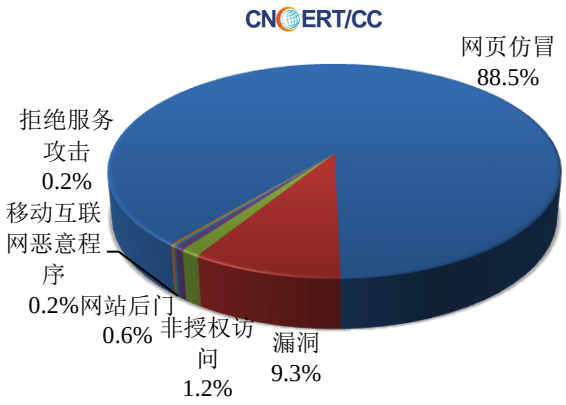
http://www.cnvd.org.cn/webinfo/list?type=4

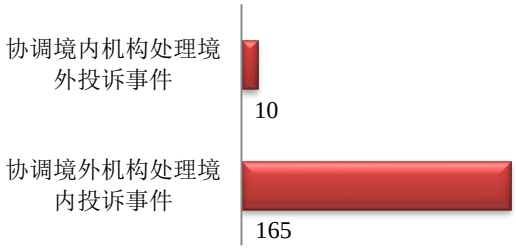
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 497 起，其中跨境网络安全事件 175 起。

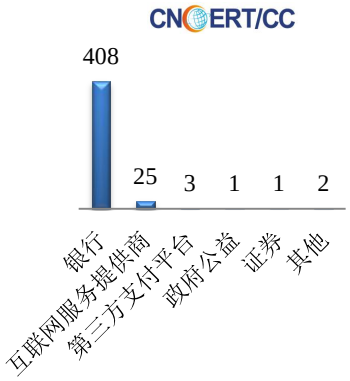
本周CNCERT处理的事件数量按类型分布
(1/15-1/21)



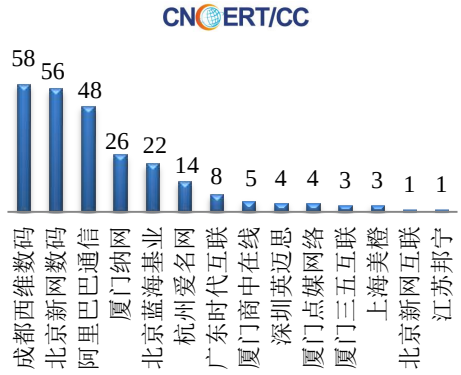


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 440 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 408 起和互联网服务提供商仿冒事件 25 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(1/15-1/21)

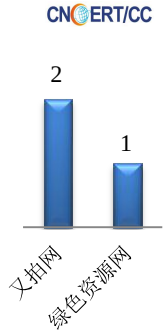


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (1/15-1/21)



本周，CNCERT 协调 2 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 3 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 (1/15-1/21)



业界新闻速递

1、正式成为法律 特朗普签署新 NSA 监控法

cnBeta.COM1 月 21 日消息 据外媒报道，当地时间 1 月 19 日，美特朗普总统宣布他已经在对《外国情报监控法（FISA）第 702 条修改再授权法》上签名，也就是说，这个备受争议的新监控条款成为法律。获悉，最新授权将在 2023 年 12 月到期。特朗普在官方声明中表示，这份法案将能让情报机构收集关于美国外的国际恐怖分子、武器扩散者及其他重要外国情报人员目标的重要情报信息。另外他还表示，比起这样一份有时间期限的法案他更希望它是永久的。据了解，这份法案于上周在众议院以 256 比 164 的投票结果通过，本周早些时候

则以 65 比 34 在参议院通过，现在总统也在上面签上了字。

2、美众议院通过《网络漏洞公开报告法案》

HackerNews.cc1 月 15 日消息 据外媒报道，本周，美国众议院通过了《网络漏洞公开报告法案(Cyber Vulnerability Disclosure Reporting Act)》。虽然这一法案的适用范围非常有限，但电子前沿基金会（EFF）对此还是表示支持并希望参议院也能为其亮绿灯。据悉，H.R.3202 是一个简短且简单的法案，由议员 Jackson Lee 发起，其将要求国土安全局（DHS）向国会提交关于政府如何处理公开漏洞的相关报告。具体点来说，报告内容分为两个部分：DHS 为协调网络漏洞公开而制定的政策和程序描述；可能为机密属性的“附件”，包括一些特定实例的描述。或许这一法案最好的地方就在于它能彰显政府确实如其长期以来所说的那样公开了大量漏洞。截止到目前，关于这方面的证据一直不多。所以假设政府有意公开报告和机密附件，那么公众对政府防御能力的信心极有可能会得到增强。

3、法德将联合向二十国集团提交比特币监管建议

新华网 1 月 20 日消息 法国经济和财政部日前提供的资料显示，法德两国将在今年 3 月向二十国集团共同提交比特币监管建议。法国经济和财政部长布鲁诺·勒梅尔与德国财政部长彼得·阿尔特迈尔 1 月 18 日日在巴黎举行了联合新闻发布会。勒梅尔说，法德双方对比特币风险有相同的担忧，对比特币监管也有同样的目标，双方将就比特币风险联合撰写分析报告及监管建议，这些成果将在今年 3 月举行的二十国集团财长会上提交给二十国集团。另据法国媒体报道，阿尔特迈尔当日在新闻发布会上说，对于比特币及其他类似货币，德法政府有共同责任向两国民众解释此类货币的风险，以及通过监管来减少风险。

4、日媒：日本将设新组织应对网络攻击 备战东京奥运

参考消息网 1 月 17 日报消息 日媒称，日本政府决定设立一个新组织，以便在民营企业受到网络攻击时，由官方和民间共享信息、了解危害程度并分享应对措施。据日本《每日新闻》1 月 14 日报道，日本政府正考虑把新组织秘书处设在内阁网络安全中心（NISC）。为方便民营企业提供受害信息，政府将采取确保匿名性的通报机制。为了加强网络安全，迎接 2020 年东京奥运会和残奥会，日本政府将在预定于 22 日召开的例行国会会议期间提交有关设立新组织的网络安全基本法修正案。报道称，民间的计算机安全公司和互联网公司将作为成员加入新组织。新组织将成为在网络攻击发生时接收信息的窗口；同时，电力和金融部门具有较大社会影响的基础设施相关企业也会被要求提供信息。NISC 等部门会把接收的信息加以归纳、分析，然后公开。政府打算建立确保匿名性的通报机制。政府还要求新组织的成员负有保守秘密的义务，将实施严格的信息管理。

5、一加承认多达 4 万名客户受到信用卡安全漏洞的影响

cnBeta.COM1 月 20 日消息 OnePlus 宣布，最近有 4 万名客户受到安全漏洞的影响，导致该公司在本周早些时候关闭了在线商店的信用卡支付。目前，第三方安全机构正在进行调查导致客户信用卡信息在购买 OnePlus 产品时被盗的漏洞。尽管在过去一周内只有信用卡信息被盗用和欺诈性购买的报道，但 OnePlus 表示，自 11 月中旬以来，盗取数据的脚本已经在其中一台支付处理服务器上运行。该脚本能够直接从客户的浏览器窗口中获取完整的信用卡信息，包括卡号，到期日期和安全代码。该公司表示，已经确定了攻击发生的地点，并已经找

到攻击者的入口点，但调查仍在进行中。OnePlus 表示，通过已经保存信息的信用卡支付的客户，通过 PayPal 处理的信用卡或通过 PayPal 账户支付的客户应该不会受到影响。

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：狄少嘉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158