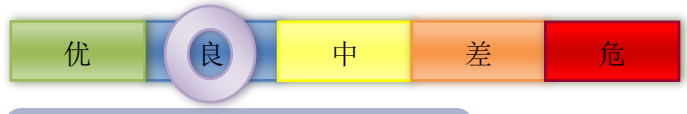
国家互联网应急中心

2018 年第 50 期

12 月 10 日-12 月 16 日

网络安全信息与动态周报

本周网络安全基本态势

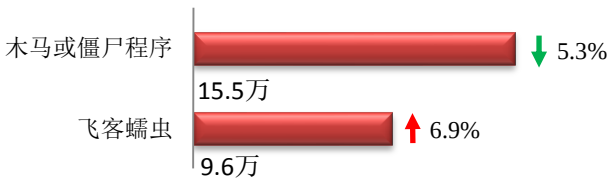


境内感染网络病毒的主机数量	•25.0万	↓ 1.0%
境内被篡改网站总数 其中政府网站数量	•806 •51	↓ 5.8% ↑ 2.0%
境内被植入后门网站总数 其中政府网站数量	•598 •4	↓ 6.3% ↓ 76.5%
针对境内网站的仿冒页面数量	•1517	↑ 56.6%
新增信息安全漏洞数量 其中高危漏洞数量	•198 •71	↓ 18.9% ↓ 34.3%

═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

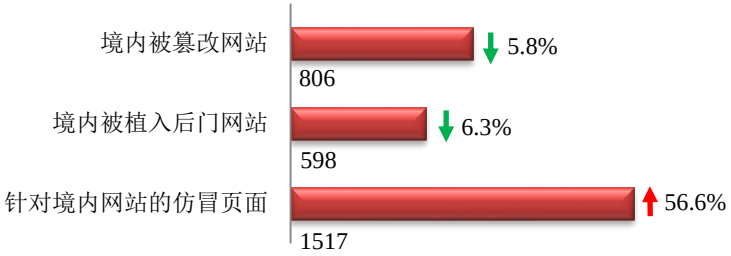
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 25.0 万个，其中包括境内被木马或被僵尸程序控制的主机约 15.5 万以及境内感染飞客（conficker）蠕虫的主机约 9.6 万。



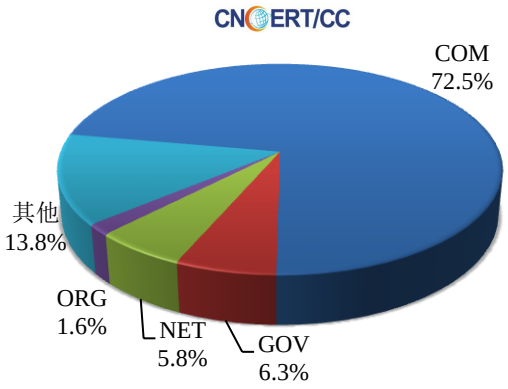
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 806 个；境内被植入后门的网站数量为 598 个；针对境内网站的仿冒页面数量 1517 个。

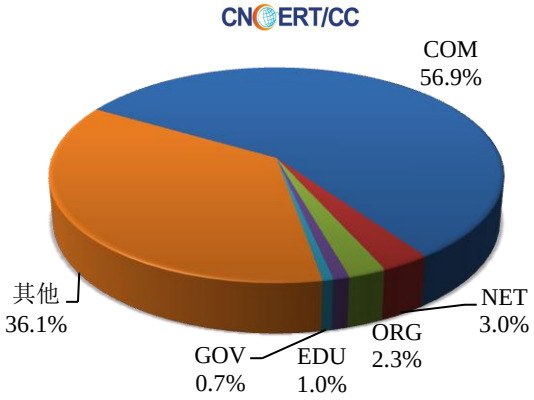


本周境内被篡改政府网站（GOV 类）数量为 51 个（约占境内 6.3%），较上周环比上升了 2.0%；境内被植入后门的政府网站（GOV 类）数量为 4 个（约占境内 0.7%），较上周环比下降了 76.5%；针对境内网站的仿冒页面涉及域名 481 个，IP 地址 253 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(12/10-12/16)

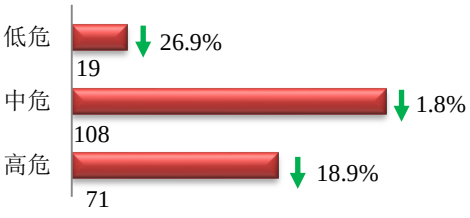


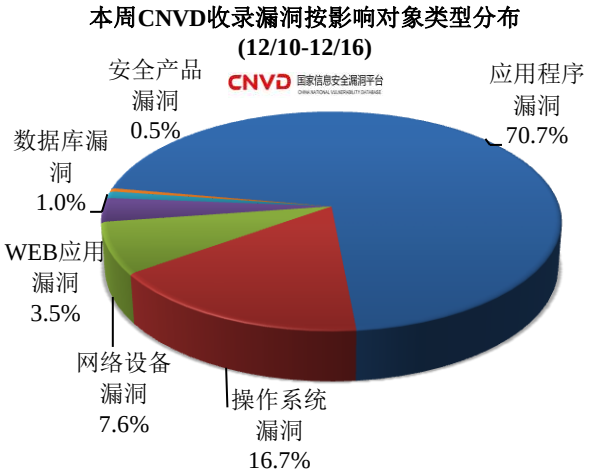
本周我国境内被植入后门网站按类型分布
(12/10-12/16)



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 198 个，信息安全漏洞威胁整体评价级别为中。





本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是操作系统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。

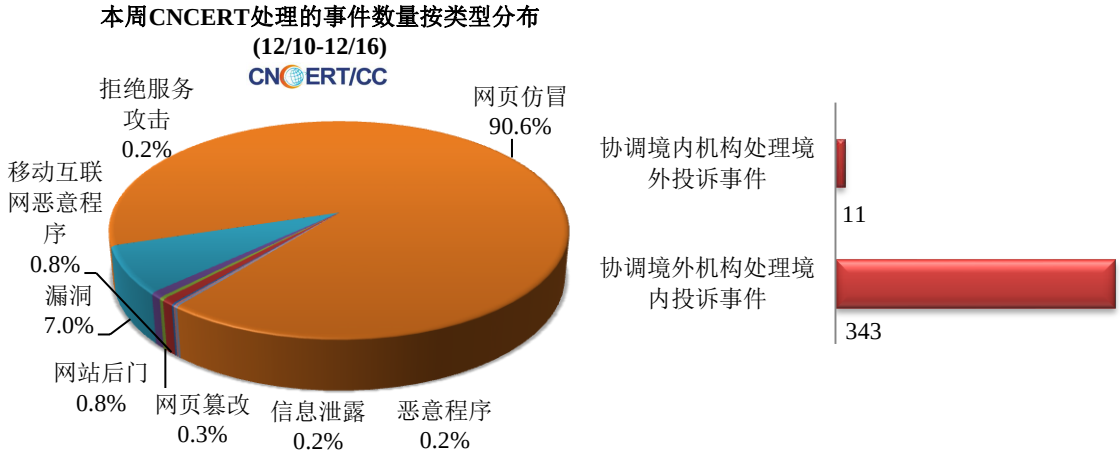
CNVD漏洞周报发布地址

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

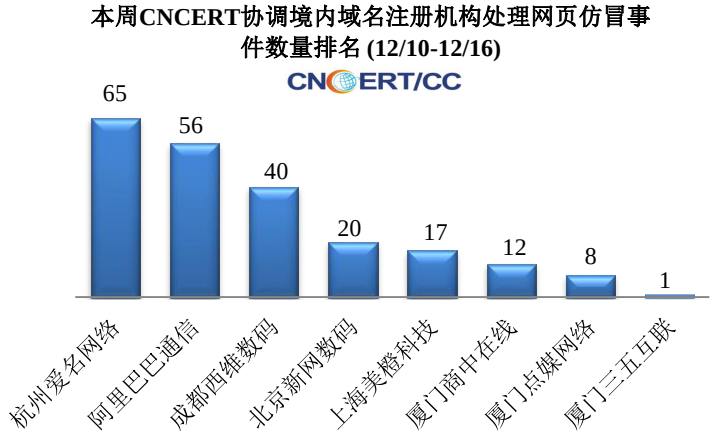
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

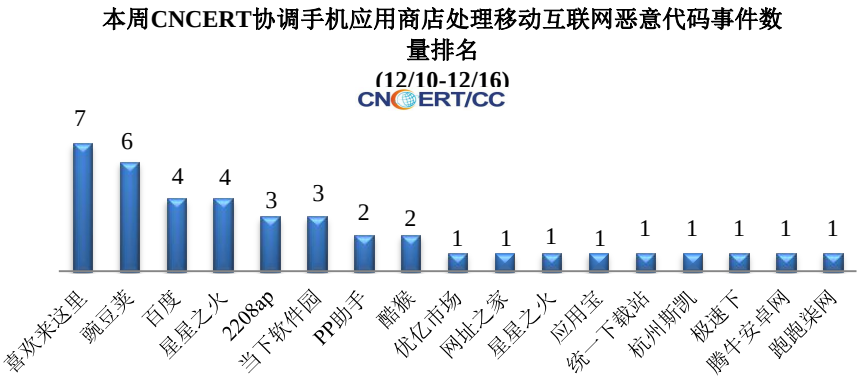
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 627 起，其中跨境网络安全事件 354 起。



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 568 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 539 起和互联网服务提供商事件 23 起。



本周，CNCERT 协调 17 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 40 个。



业界新闻速递

1、欧盟达成有关网络安全法的政策协议

安全内参 12 月 13 日消息 欧洲议会、欧盟理事会和欧盟委员会就网络安全法达成了一项政策协议，该法案加强了欧盟网络安全机构——欧盟网络和信息安全局（ENISA）的授权，以更好地支持成员国应对网络安全威胁和攻击。该法案还建立了欧盟的网络安全认证框架，增强了在线服务和消费者设备的网络安全。据欧盟委员会网站 2018 年 12 月 10 日反映，布鲁塞尔当地时间 12 月 10 日晚上，欧洲议会、欧盟理事会和欧盟委员会就网络安全法达成了一项政策协议，该法案加强了欧盟网络安全机构——欧盟网络和信息安全局（ENISA）的授权，以更好地支持成员国应对网络安全威胁和攻击。该法案还建立了欧盟的网络安全认证框架，增强了在线服务和

消费者设备的网络安全。

2、澳大利亚通过全球首项反加密立法

E 安全 12 月 11 日消息 根据澳大利亚的新法律，安全机构将获取更多加密信息的访问权限。该法案将迫使苹果、脸书与谷歌等科技公司解除加密保护以允许调查人员跟踪恐怖分子及其他罪犯的通信。而这项措施是极具争议的。澳大利亚在周四刚通过的法律强制要求科技公司、设备制造商与服务供应商内置警方所需要的功能，以破解现有的这些秘密代码。然而，企业若担心“系统性弱点”，即这些功能可能导致其他用户的安全性受损，则可不应用这些功能。 此次澳大利亚立法是全球首例此类立法。

3、意大利石油与天然气服务公司 Saipem 遭遇网络攻击

E 安全 12 月 14 日消息 意大利石油与天然气服务公司 Saipem 的客户遍及全球 60 余个国家，沙特阿拉伯石油与天然气巨头沙特阿美公司（Saudi Aramco）也是其客户之一。众多威胁者通常将 Saipem 视为战略目标。 周一在印度发现了此次攻击，而此次攻击的“重灾区”主要位于沙特阿拉伯、阿拉伯联合酋长国与科威特等中东国家。其位于意大利、法国与英国的主要运营中心不受此次攻击影响。

4、法国外交部网站遭入侵 出境旅客信息被泄露

cnbeta.COM 12 月 14 日消息 法国外交部 13 日发布公告，外交部网站近日遭非法入侵，部分法国出境旅客在注册时填写的个人信息被泄露。外交部“阿丽亚娜”服务平台近日遭黑客非法入侵，致该国部分出境游客的个人信息被泄露。但这些信息并不包含已注册用户的敏感数据、个人金融信息，或可能透露旅客目的地的相关信息。法国外交部表示已立即采取措施避免同类事件再次发生，并以发送邮件、手机信息等方式通知相关人员。法国外交部还责成国家信息与自由委员会通过司法手段处理本次信息泄露事件。法国外交部呼吁已注册“阿丽亚娜”服务平台的用户对可疑来源的信息保持警惕，并表示这一事件不会影响该平台的可靠性。

5、5200 万用户数据泄露 谷歌将提前 4 个月关闭 Google+

新浪科技 12 月 11 日消息 谷歌表示，将于明年 4 月关闭 Google+社交媒体服务，比原计划提前 4 个月。此前，该公司今年第二次发现 Google+的软件漏洞，新漏洞导致合作伙伴应用能访问用户的个人数据。不过谷歌在博客中表示，没有发现任何证据表明，其他应用使用该漏洞访问了这些数据，包括用户的姓名、电子邮件地址、性别和年龄。谷歌表示，在上月引入的 6 天时间内，该漏洞影响了 5250 万个 Google+帐号，其中包括一些企业客户的帐号。今年 10 月，谷歌表示，将于 2019 年 8 月关闭 Google+的消费级版本，因为维护该服务带来了太大的挑战。当时该公司表示，来自 50 万用户的个人信息数据可能被一个已经存在两年多的漏洞泄露给合作伙伴应用。

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：徐原

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158