国家互联网应急中心

网络安全信息与动态周报

2019 年第 3 期

1 月 14 日-1 月 20 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	•21.1万	↑9.6%
境内被篡改网站总数 其中政府网站数量	•638 •43	↓7.5% ↑4.9%
境内被植入后门网站总数 其中政府网站数量	•561 •9	↓30.3% ↓47.1%
针对境内网站的仿冒页面数量	•1718	↓52.7%
新增信息安全漏洞数量 其中高危漏洞数量	•375 •110	↑66.7% ↑61.8%

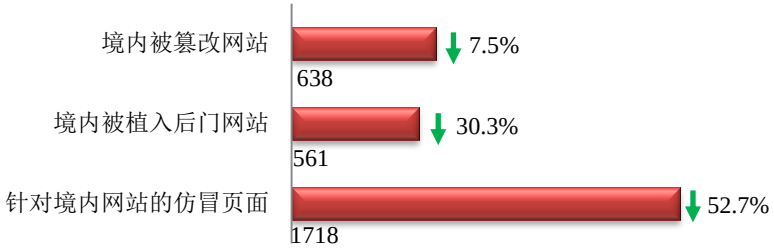
=表示数量与上周相同　↑表示数量较上周环比增加　↓表示数量较上周环比减少

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 21.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 12.4 万以及境内感染飞客（conficker）蠕虫的主机约 8.7 万。

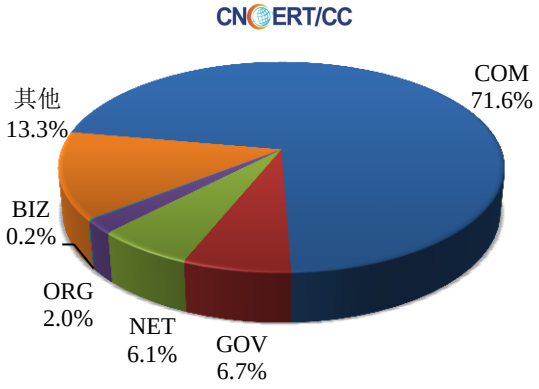
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 638 个；境内被植入后门的网站数量为 561 个；针对境内网站的仿冒页面数量 1718 个。

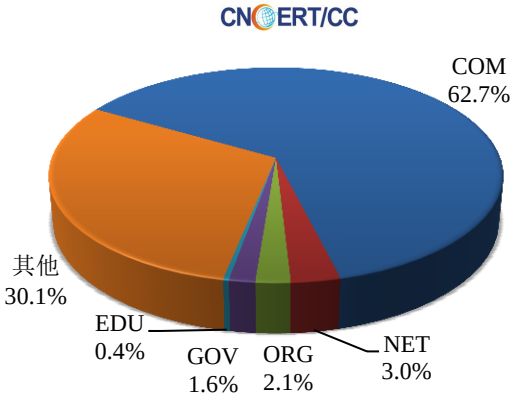


本周境内被篡改政府网站（GOV 类）数量为 43 个（约占境内 6.7%），较上周环比上升了 4.9%；境内被植入后门的政府网站（GOV 类）数量为 9 个（约占境内 1.6%），较上周环比下降了 47.1%；针对境内网站的仿冒页面涉及域名 412 个，IP 地址 221 个，平均每个 IP 地址承载了约 109 个仿冒页面。

本周我国境内被篡改网站按类型分布
(1/14-1/20)

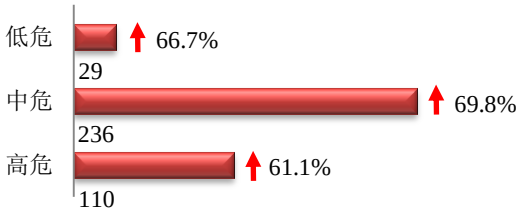


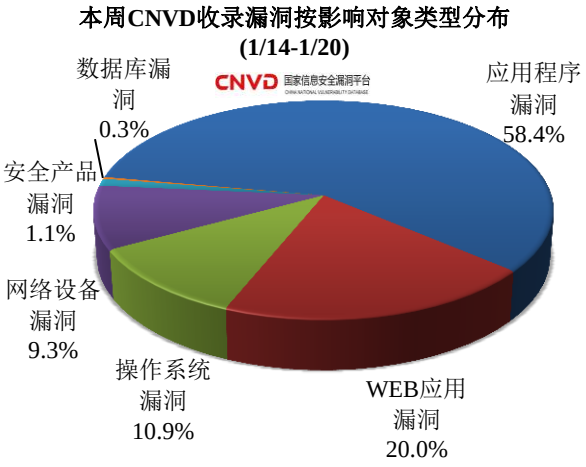
本周我国境内被植入后门网站按类型分布
(1/14-1/20)



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 375 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 WEB 应用程序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。

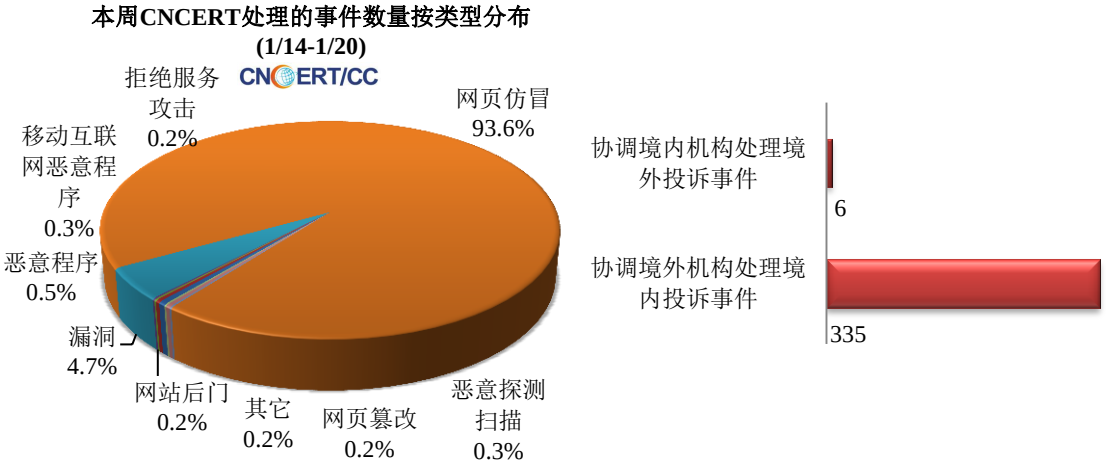
CNVD漏洞周报发布地址

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。

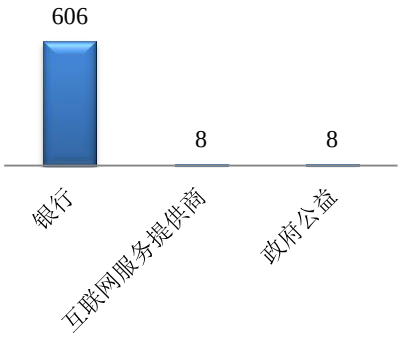
本周事件处理情况

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 658 起，其中跨境网络安全事件 341 起。

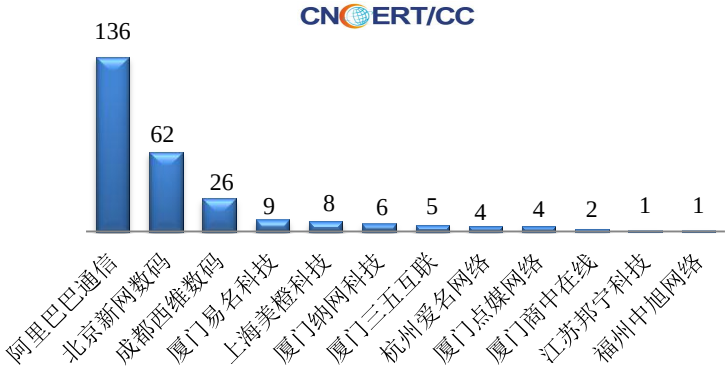


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 616 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 606 起和互联网服务提供商仿冒事件 8 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (1/14-1/20)

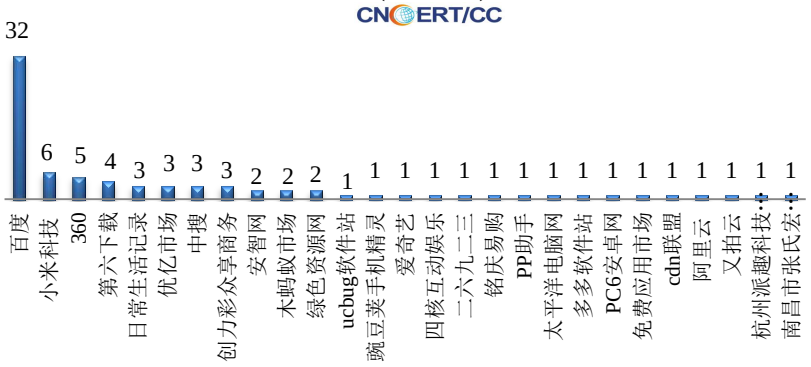


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (1/14-1/20)



本周，CNCERT 协调 27 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 81 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 (1/14-1/20)



业界新闻速递

1、澳大利亚将加强 GPS 基础设施网络防御

E 安全 1 月 19 日消息 澳大利亚地球科学局（Geoscience Australia）非常重视 SBAS（Satellite-based Augmentation System，星基增强系统）项目的复原能力，计划制定具体的网络安全战略以应对内在风险。网络安全战略的重点是测试两种新的卫星定位技术，即下一代 SBA 和精确点定位技术。该战略将就如何保障 SBAS 地面基础设施和处理设施的安全提供信息和建议。SBAS 项目于 2018 年获得 1.61 亿美元的预算，旨在推动 GPS 和 Galileo 在整个澳大利亚及其海域的卫星定位能力达到分米级精度。提高卫星定位能力可提高智能导航工具的导航能力，海上遇险船只的定位精度，以及农场的用水效率等。地球科学局目前在一个 SBAS 实验台进行一些实验，实验预计将在本月底之前完成。

2、法国泰雷兹集团成立埃布韦尔网络安全研究基地

安全内参 1 月 15 日消息 国泰雷兹集团斥资 2000 万英镑，将在英国南威尔士建立一个研发中心。集团已在英国其他 12 个地区运营业务，涉及国防、航空航天和运输等。埃布韦尔中心将成为数字安全创新的实验基地。该中心将为该地区的复兴提供催化剂。第一批工作人员共 11 人，计划将于 2 月开始工作。到 2021 年，该中心将全面运营。其中泰雷兹集团参与开发复杂的电气系统，这些系统可用于防空系统到网络安全的所有领域。国家数字开发中心（NDEC）也将与南威尔士大学合作。该项目也获得了威尔士政府的支持，建设工作将于春季开始。埃布韦尔中心将致力于保护发电站、铁路、水利、电信和空中交通管制安全的系统。该中心将有助于威尔士把握数字转型的全球机遇，为开拓性的研究提供基础，并为不同形式和规模的企业提供所需的技能和知识。

3、韩国国防部机密文件被盗

E 安全 1 月 18 日消息 有黑客入侵了韩国一家政府机构的电脑系统，该机构负责韩国军方的武器和弹药采购。韩国政府表示，黑客入侵了 30 台电脑，并从 10 台电脑中窃取了数据。黑客攻击发生于 2018 年 10 月。韩国媒体报道，被入侵的组织是韩国国防部下属的国防采购项目管理局（DAPA）。被盗文件包含了下一代战斗机的采购信息。去年 11 月，大韩民国国家情报院（NIS,National Intelligence Service）调查了这起网络攻击事件，并向政府报告了调查结果，政府本周向公众披露了这起网络攻击事件。

4、Amadeus 订票系统惊曝高危漏洞：影响全球近半数航企

cnBeta.COM1 月 17 日消息 全球近半数国际航空公司所使用的 Amadeus 机票预订系统，近日被曝存在一个严重的安全漏洞，使得黑客能够轻松查看和更改旅客信息。比如将其他常旅客的里程兑换到黑客指定的个人账户，或更改联系人信息、将客户机票退订。据悉，该漏洞由 Noam Rotem 与安全侦探研究实验室发现，影响全球 141 家国际航空公司（占比 44%）。Rotem 展示可通过 PNR 代码更改任何乘客的航班信息。漏洞与乘客姓名记录（PNR）系统有关，PNR 用于给航班上的每位乘客指定唯一标识符。通过刷新机票预订网页的特定元素（RULE_SOURCE_1_ID），Rotem 能够查看他被 Amadeus 纪录任何客户的 PNR 名称和航班详情。

5、菲律宾金融服务公司数据泄露 影响 90 万客户

凤凰科技网 1 月 20 日消息 菲律宾金融服务提供商 Cebuana Lhuillier 表示，大约有 90 万名客户的数据在未经授权情况下遭黑客窃取，该公司已向有关部门报警并介入这一事件的调查。此次泄密事件发生，正值菲律宾调查人员针对菲外交部长指控黑客入侵该国护照数据库展开调查之际。上周，菲外交部长指控称，一家私人承包的公司从外交部的护照数据库中窃取了文件和数据。

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：朱芸茜

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158