国家互联网应急中心

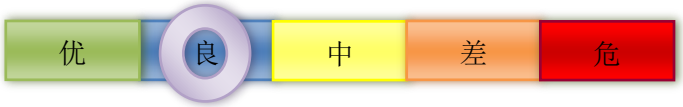
网络安全信息与动态周报

2018 年第 46 期

11 月 12 日-11 月 18 日

CNCERT/CC

本周网络安全基本态势

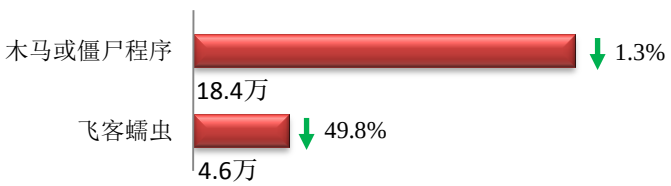


境内感染网络病毒的主机数量	•23.0万	↓ 17.3%
境内被篡改网站总数 其中政府网站数量	•537 •26	↑ 15.2% ↓ 38.1%
境内被植入后门网站总数 其中政府网站数量	•613 •14	↓ 5.0% ↑ 40.0%
针对境内网站的仿冒页面数量	•1783	↑ 25.8%
新增信息安全漏洞数量 其中高危漏洞数量	•202 •100	↑ 17.4% ↑ 42.9%

═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

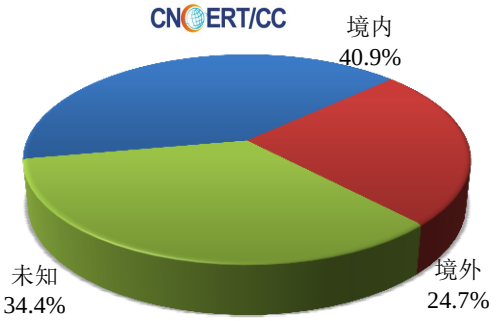
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 23.0 万个，其中包括境内被木马或被僵尸程序控制的主机约 18.4 万以及境内感染飞客（conficker）蠕虫的主机约 4.6 万。

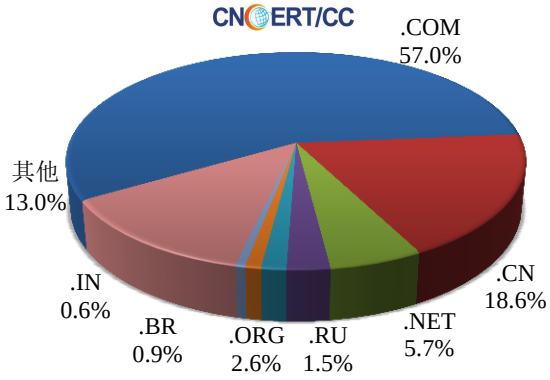


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 3381 个，涉及 IP 地址 5946 个。在 3381 个域名中，有 24.7%为境外注册，且顶级域为.com 的约占 57.0%；在 5946 个 IP 中，有约 51.1%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 500 个 IP。

本周放马站点域名注册所属境内外分布
(11/12-11/18)



本周放马站点域名所属顶级域的分布
(11/12-11/18)



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。

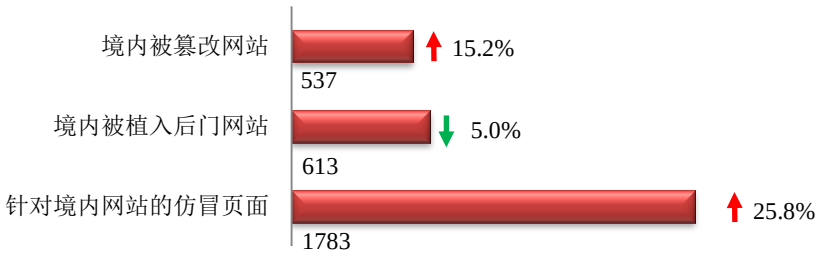
ANVA恶意地址黑名单发布地址

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。

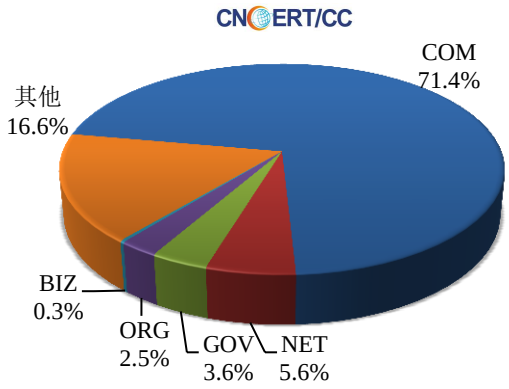
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 537 个；境内被植入后门的网站数量为 613 个；针对境内网站的仿冒页面数量为 1783 个。

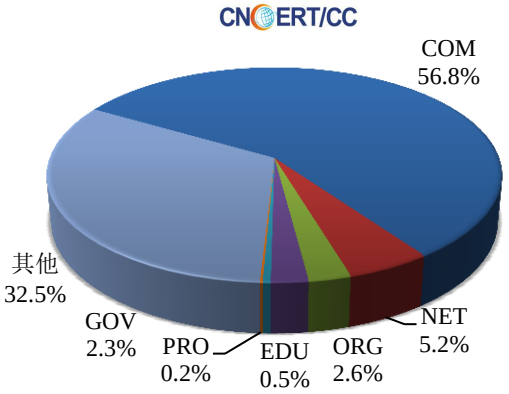


本周境内被篡改政府网站（GOV 类）数量为 26 个（约占境内 4.8%），较上周环比下降了 38.1%；境内被植入后门的政府网站（GOV 类）数量为 14 个（约占境内 2.3%），较上周环比上升了 40.0%；针对境内网站的仿冒页面涉及域名 522 个，IP 地址 283 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(11/12-11/18)

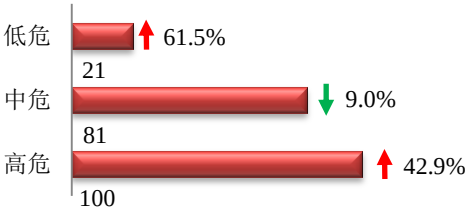


本周我国境内被植入后门网站按类型分布
(11/12-11/18)

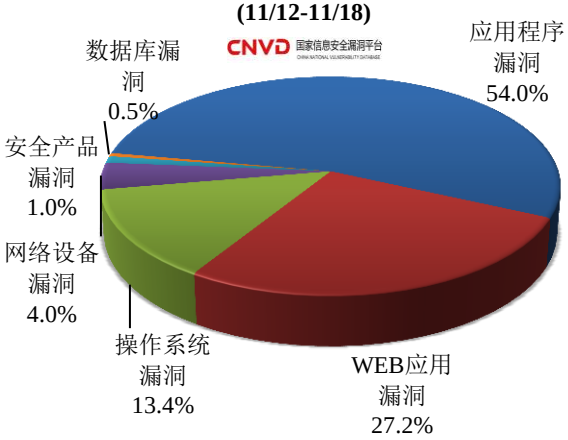


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 202 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
(11/12-11/18)



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

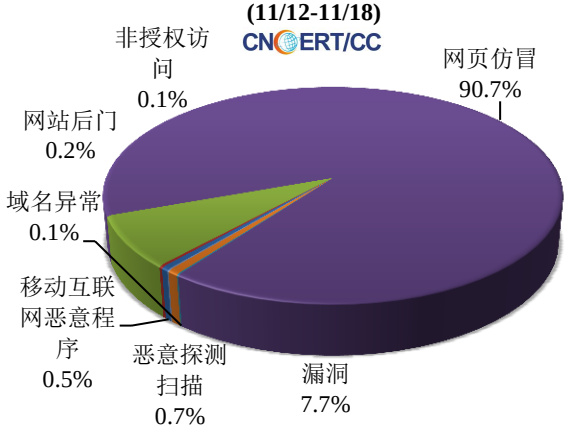
http://www.cnvd.org.cn/webinfo/list?type=4

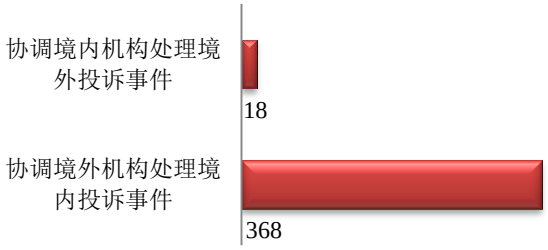
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 846 起，其中跨境网络安全事件 386 起。

本周CNCERT处理的事件数量按类型分布 (11/12-11/18)

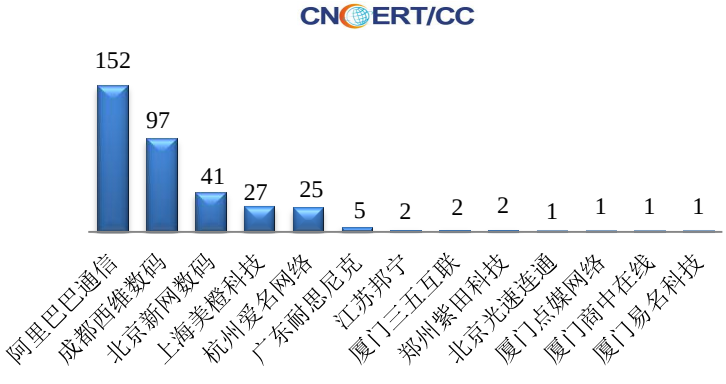




本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 767 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 714 起和互联网服务提供商仿冒事件 28 起。

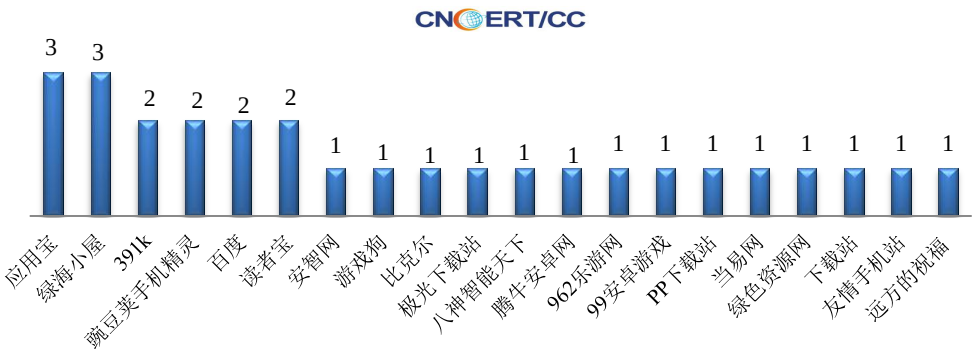
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (11/12-11/18)

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 (11/12-11/18)



本周，CNCERT 协调 20 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 28 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 (11/12-11/18)



业界新闻速递

1、国会通过法案，将在美国国土安全部创建网络安全机构

E 安全 11 月 16 日消息 美国众议院（U.S. House of Representatives）通过一项法案，将在美国国土安全部（简称 DHS）创建一个新的网络安全机构。网络安全与基础设施安全局（简称 CISA）法案已于 10 月获参议院通过，再经总统签字便可成为法律。国会一致通过了立法。该法案将国家保护与计划局（简称 NPPD）重组为网络安全与基础设施安全局（简称 CISA），并由 CISA 负责网络与物理基础设施安全。

2、英国隐私保护组织投诉甲骨文等企业违反欧盟 GDPR 政策

新浪科技讯 11 月 14 日消息，据中国台湾地区 iThome.com.tw 报道，英国非营利隐私保护组织 Privacy International（PI）上周投诉包括甲骨文（Oracle）在内的 7 家企业违反《欧盟通用数据保护条例》（EU General Data Protection Regulation，GDPR），并督促法国、英国及爱尔兰的数据保护组织展开调查。据报道，受到投诉的 7 家企业全都握有大量消费者资料，包括从事数据分析的甲骨文与 Acxiom，提供广告服务的 Criteo、Quantcast、Tapad，以及信用报告企业 Equifax 与 Experian。

3、南非正式通过《网络犯罪和网络安全法案》

人民网 11 月 14 日消息 南非议会司法委员会正式通过了《网络犯罪和网络安全法案（Cybercrimes and Cybersecurity Bill）》。该法案自 2017 年首次提出，经过多次重大修改，旨在

让南非与其他国家的网络法律接轨，应对不断增长的网络犯罪趋势。该法案规定，任何人违反其中的一项规定，一旦被判定有罪，将面临罚款和（或）不超过三年的监禁。]

4、代号“沙欣行动”：美安全公司揭露针对巴基斯坦空军的间谍活动

黑客视界 11 月 15 日消息 美国网络安全公司 Cylance 于本周一揭露了一场以巴基斯坦空军成员为目标的网络间谍活动。它的代号为“沙欣行动（Operation Shaheen）”，疑似由某个国家黑客组织发起。作为“沙欣行动”的一部分，“白衣公司”的黑客针对巴基斯坦空军成员实施了鱼叉式网络钓鱼攻击，诱饵文件的命名参考了一些大事件、政府文件，以及目标可能感兴趣的新闻文章（如巴基斯坦空军、巴基斯坦政府、中国驻巴基斯坦军事和顾问等）。

5、超过 2 万张银行卡数据在暗网兜售，几乎涵盖巴基斯坦国内所有银行

cnBeta.COM11 月 13 日消息 据巴基斯坦 GEO 电视台报道，几乎所有巴基斯坦银行在最近都受到了黑客入侵的影响，而这一令人震惊的消息已经在上周得到了巴基斯坦联邦调查局（FIA）网络犯罪部门负责人的证实。FIA 已向该国所有银行通报了调查结果，并要求与其代表进行会谈，以便对此事件做出回应，减少损失并提高巴基斯坦银行的整体安全性。从最近的报道来看，巴基斯坦国内银行的安全现状确实亟待改善。在上周针对伊斯兰银行的网络攻击中，攻击者至少盗走了 260 万卢比。巴基斯坦计算机应急响应中心（PakCERT）发布了一份报告，详细描述了数据泄露的时间和规模。PakCERT 的专家认为，这些数据是通过银行客户的刷卡行为获得的。这些支付卡数据正在暗网出售，售价从 100 美元至 160 美元不等。

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：严寒冰

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158