国家互联网应急中心

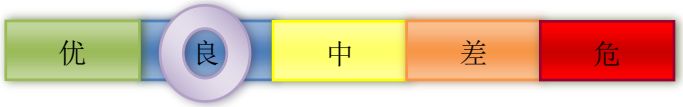
网络安全信息与动态周报

2018 年第 45 期

11 月 5 日-11 月 11 日

CNCERT/CC

本周网络安全基本态势

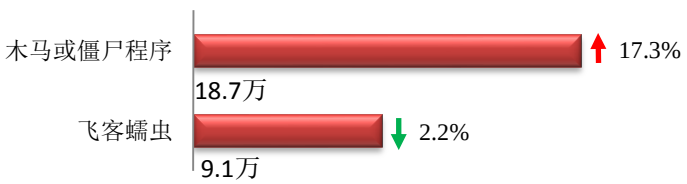


境内感染网络病毒的主机数量	•27.8万	↑ 10.1%
境内被篡改网站总数 其中政府网站数量	•466 •42	↑ 90.2% ↑ 110.0%
境内被植入后门网站总数 其中政府网站数量	•645 •10	↓ 27.1% ↑ 11.1%
针对境内网站的仿冒页面数量	•1417	↑ 9.8%
新增信息安全漏洞数量 其中高危漏洞数量	•172 •70	↓ 15.3% ↓ 22.2%

═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

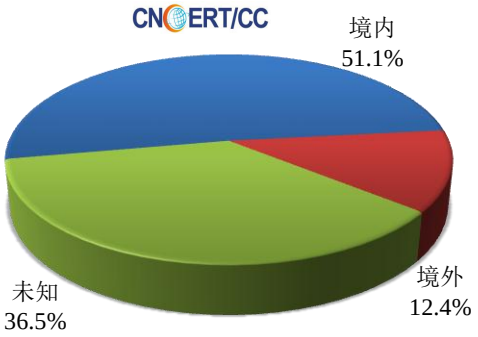
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 27.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 18.7 万以及境内感染飞客（conficker）蠕虫的主机约 9.1 万。

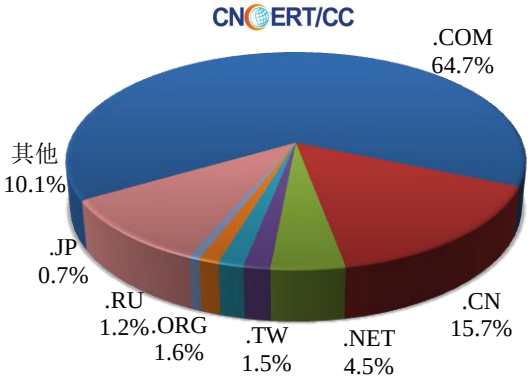


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 5573 个，涉及 IP 地址 6186 个。在 5573 个域名中，有 12.4%为境外注册，且顶级域为.com 的约占 64.7%；在 6186 个 IP 中，有约 52.7%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 579 个 IP。

本周放马站点域名注册所属境内外分布
(11/5-11/11)



本周放马站点域名所属顶级域的分布
(11/5-11/11)



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。

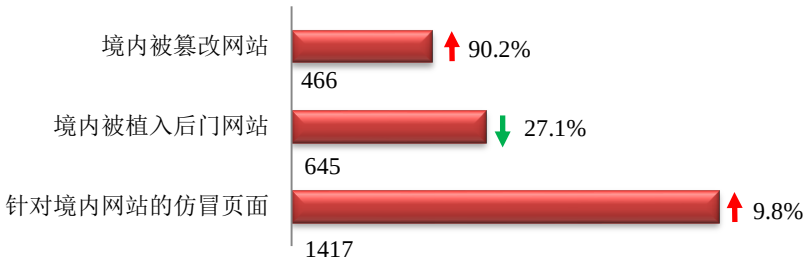
ANVA恶意地址黑名单发布地址

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。

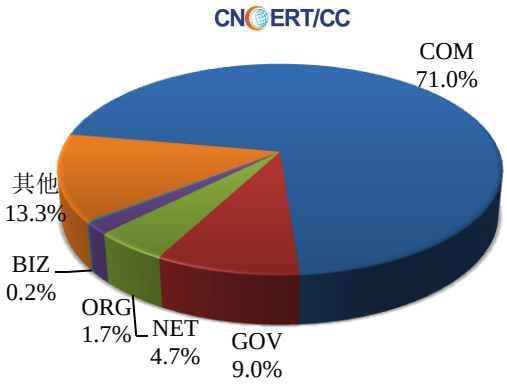
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 466 个；境内被植入后门的网站数量为 645 个；针对境内网站的仿冒页面数量为 1417 个。

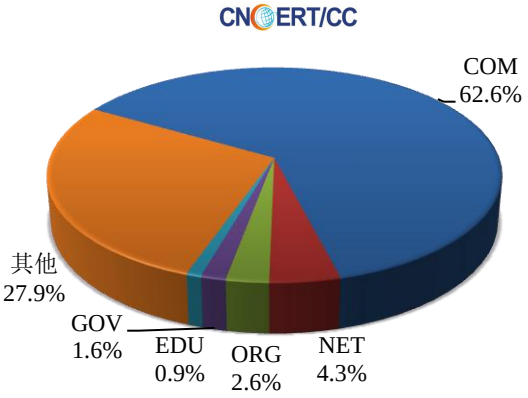


本周境内被篡改政府网站（GOV 类）数量为 42 个（约占境内 9.0%），较上周环比上升了 110.0%；境内被植入后门的政府网站（GOV 类）数量为 10 个（约占境内 1.6%），较上周环比下上升了 11.1%；针对境内网站的仿冒页面涉及域名 417 个，IP 地址 228 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(11/5-11/11)

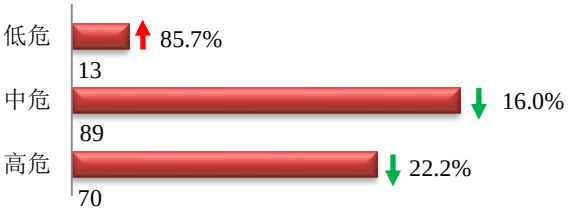


本周我国境内被植入后门网站按类型分布
(11/5-11/11)

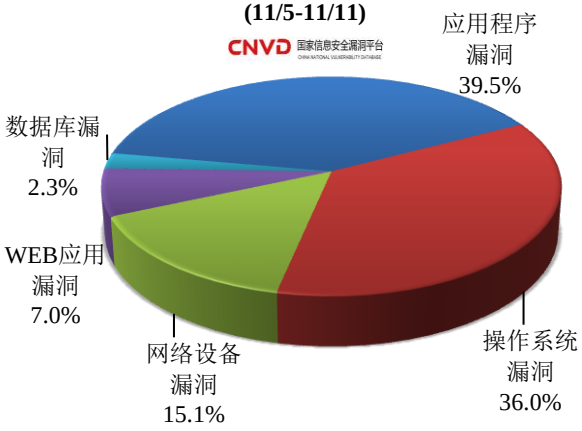


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 172 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
(11/5-11/11)



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

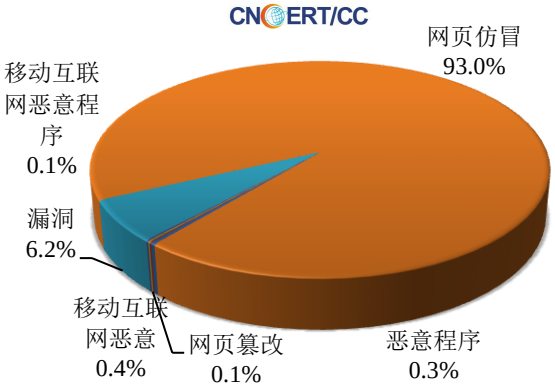
http://www.cnvd.org.cn/webinfo/list?type=4

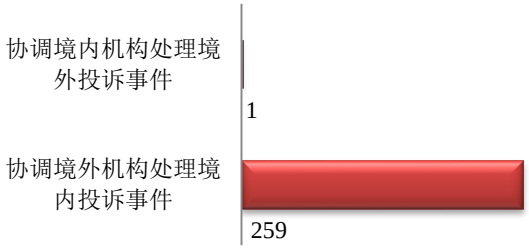
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 705 起，其中跨境网络安全事件 260 起。

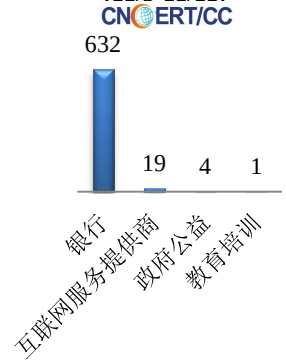
本周CNCERT处理的事件数量按类型分布 (11/5-11/11)



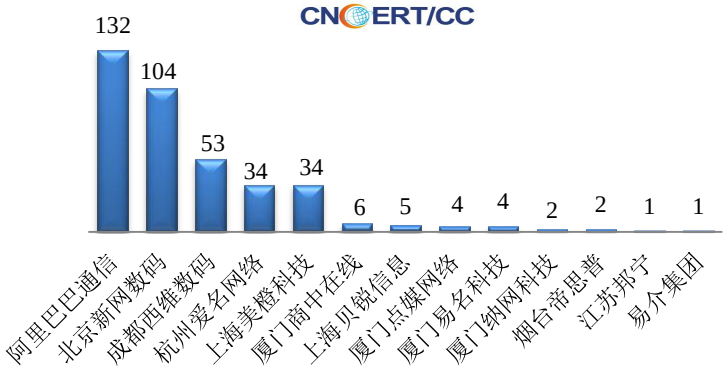


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 656 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 632 起和互联网服务提供商仿冒事件 19 起。

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

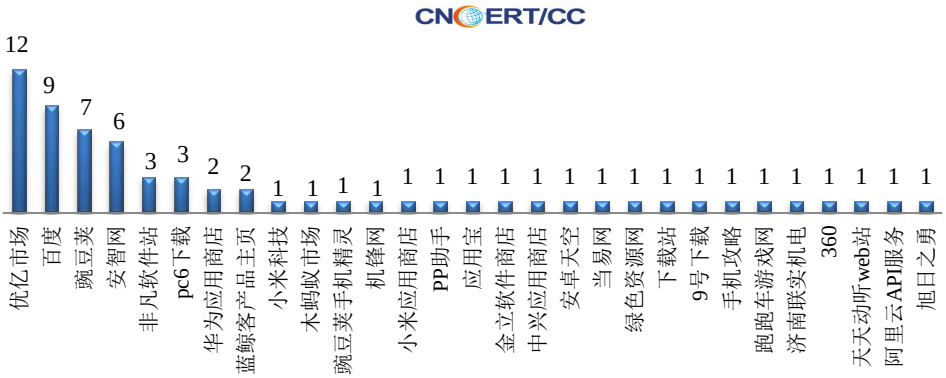


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (11/5-11/11)



本周，CNCERT 协调 29 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 65 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 (11/5-11/11)



业界新闻速递

1、50 个国家签署文件承诺将打击网络犯罪行为

cnBeta.COM 11 月 13 日消息 据外媒报道，来自世界各地 50 个国家和超 150 多家科技公司签署了一项名为《Paris call for trust and security in cyberspace》的承诺以表它们致力于打击网络犯罪行为的决心。获悉，法国总统马克龙在众领导人参加一战结束 100 周年纪念活动前一日公布了这份文件。签署该文件的国家有日本、加拿大和所有欧盟国家，谷歌、微软、Facebook 等国际科技巨头公司也表示将致力于打击网络犯罪。虽然美国大量政府机构和官员近些年来表示国家经历了多起网络犯罪案件包括 2016 年总统大选干预等，但它并没有在这份文件上签字。另外，中国和俄罗斯也没有在这份文件上签字。

2、美国空军宣布第三次 Bug 赏金计划

E 安全 11 月 8 日消息 美国空军联合 HackerOne 推出第三次 Bug 赏金计划。“黑掉空军 3.0（Hack the Air Force 3.0）”是由美国政府管理的、迄今规模最大的 Bug 赏金计划，范围包括 191 个国家，持续时间逾 4 周。该项目于 10 月 19 日启动，将于 11 月 22 日前结束。600 名已注册的研究人员将受邀在美国国防部应用程序中查找漏洞，最近该应用程序已迁移至美国空军管理的云环境。约 70%参赛者将根据候选人 HackerOne 声誉得分选出，剩余 30%参赛者将通过随机抽取方式选出。空军首席信息安全官万达·琼斯·希思（WandaJones-Heath）表示，“安全漏洞对空军网络造成严重威胁，‘黑掉空军 3.0’表明了空军想要修复这些漏洞的诚意。”第一次

“黑掉空军”生成逾 200 份有效漏洞报告，研究人员所获赏金超过 13 万美元。第二次“黑掉空军”计划中，27 名白帽黑客发现 106 个漏洞，国防部向其支付逾 10 万美元赏金。最近，国防部通知 bug 赏金猎人，其将针对国防部高价值资产开展一整年的“入侵国防部（Hack the Pentagon）”计划。该计划由众包安全测试平台 Bugcrowd 承办。

3、脸书账户被黑，8.1 万用户私人信息待售

E 安全 11 月 6 日消息 据英国广播公司（BBC）对事情进展的报道：黑客已非法访问约 1.2 亿脸书用户的账户及其私人信息。据报道，脸书数据外泄用户主要来自乌克兰和俄罗斯，但也有大量来自英国、美国、巴西及其他地方的用户数据外泄。据称，今年九月首次发现这一漏洞，当时，其中一名黑客在论坛发布了出售被盗数据的广告。另一方面，这些脸书用户的消息详细信息是在其下载了恶意浏览器扩展程序后遭窃的，该程序挖出了这些用户的账号详细信息。该报道补充道，这些黑客以 10 美分每个账号的价格出售从脸书账号所窃取的全部信息的访问权。虽然肇事者告诉英国广播公司俄语服务小组，其“数据库包含 1.2 亿账户”，但目前该数目尚并未获外部网络安全专家证实。

4、汇丰银行再次身陷数据泄露，部分客户个人信息被窃取

黑客视界 11 月 8 日消息 据外媒报道，汇丰银行（HSBC Bank）似乎再一次成为了数据泄露事件的受害者，部分客户的个人和财务信息已经被证实能够被入侵者所访问，这包括客户的全名、邮寄地址、电话号码、电子邮箱地址、出生日期、帐户号码、帐户类型、帐户余额、交易历史、收款人帐户信息和帐单历史记录。从汇丰银行在上周五（11 月 2 日）向加利福利亚洲总检察长办公室提交的一份新的数据泄露通知来看，汇丰银美国（HSBC Bank USA）部分客户的网上银行账户在 2018 年 10 月 4 日至 2018 年 10 月 14 日期间遭到了未经授权的访问。目前，汇丰银行美国公司已经表示，它已经通过了所有受影响的客户，并将为他们提供为期一年的 Identity Guard 信用监控服务。Identity Guard 不仅能够为用户提供必要的信用监控，而且还会就可疑的身份盗用活动向用户发出提醒。

5、英特尔超线程 CPU PortSmash 漏洞曝光，可获取加密数据

E 安全 11 月 7 日 英特尔超线程 CPU PortSmash 漏洞曝光，可允许攻击者从同一 CPU 内核中获取其他进程中的加密数据，包括密码、加密密钥等。该漏洞由芬兰坦佩雷理工大学和古巴哈瓦那大学的研究人员发现，被追踪为 CVE-2018-5407，已加入去年列出的边通道漏洞列表，一起加入该列表的包括 Meltdown、Spectre、TLBleed 和 Foreshadow 漏洞等。由于同步多线程（SMT）可将处理器的每个物理内核分成虚拟内核（线程）来工作，且允许在同一物理内核中并行运行两个线程来提高性能，因此，攻击者可在同一 CPU 内核中与特定进程同时运行恶意进程，允许 PortSmash 代码测量每个操作所花费的精确时间来确认特定进程执行的操作。

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：刘晓敏

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158