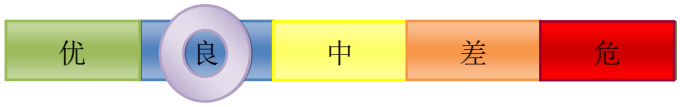
国家互联网应急中心

2018 年第 42 期

10 月 15 日-10 月 21 日

网络安全信息与动态周报

本周网络安全基本态势

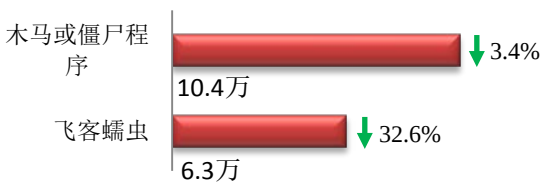


境内感染网络病毒的主机数量	•16.7万	17.0%
境内被植入后门网站总数 其中政府网站数量	•773 •10	31.7% =
针对境内网站的仿冒页面数量	•1052	48.5%
新增信息安全漏洞数量 其中高危漏洞数量	•244 •101	1.7% 18.8%

=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

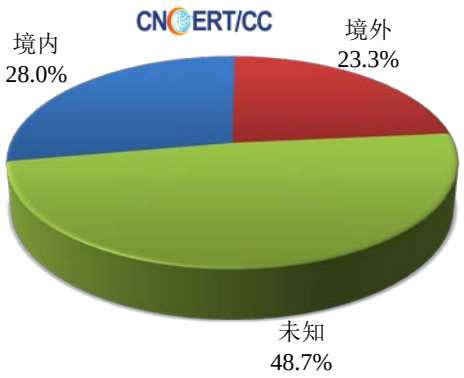
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 16.7 万个，其中包括境内被木马或被僵尸程序控制的主机约 10.4 万以及境内感染飞客（conficker）蠕虫的主机约 6.3 万。

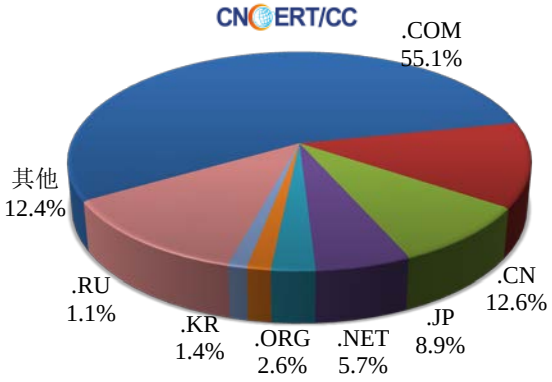


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 6466 个，涉及 IP 地址 82788 个。在 6466 个域名中，有 23.3%为境外注册，且顶级域为.com 的约占 55.1%；在 82788 个 IP 中，有约 31.9%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 579 个 IP。

本周放马站点域名注册所属境内外分布
(10/15-10/21)



本周放马站点域名所属顶级域的分布
(10/15-10/21)



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。

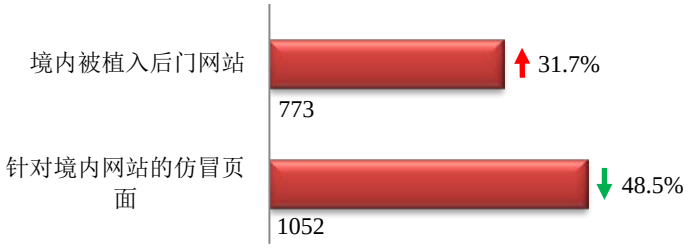
ANVA恶意地址黑名单发布地址

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。

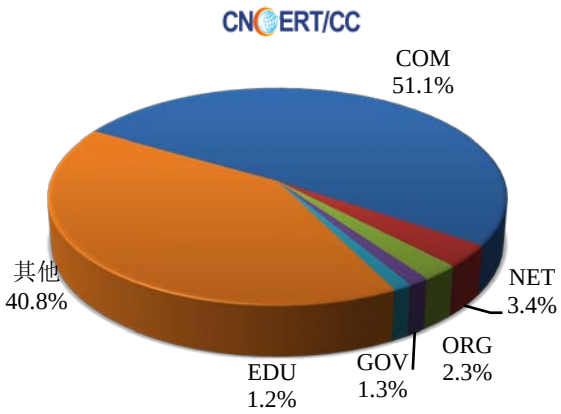
本周网站安全情况

本周 CNCERT 监测发现境内被植入后门的网站数量为 773 个；针对境内网站的仿冒页面数量为 1052。



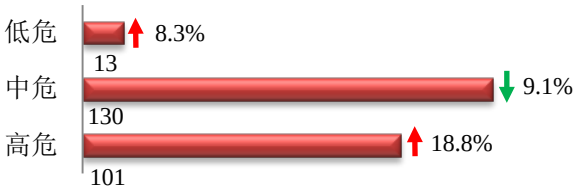
本周境内被植入后门的政府网站（GOV 类）数量为 10 个（约占境内 1.3%）；针对境内网站的仿冒页面涉及域名 318 个，IP 地址 211 个，平均每个 IP 地址承载了约 4 个仿冒页面。

本周我国境内被植入后门网站按类型分布
(10/15-10/21)

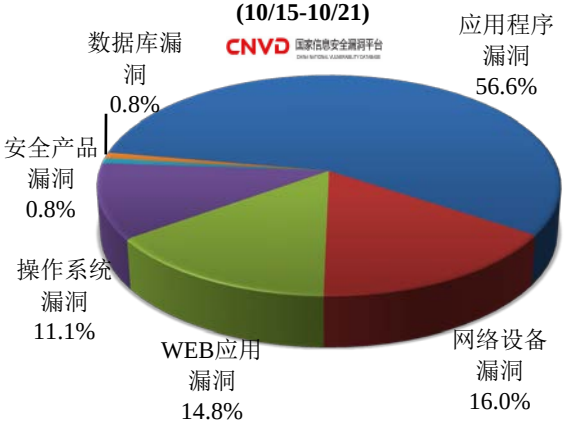


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 244 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
(10/15-10/21)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是网络设备漏洞和 WEB 应用漏洞。

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

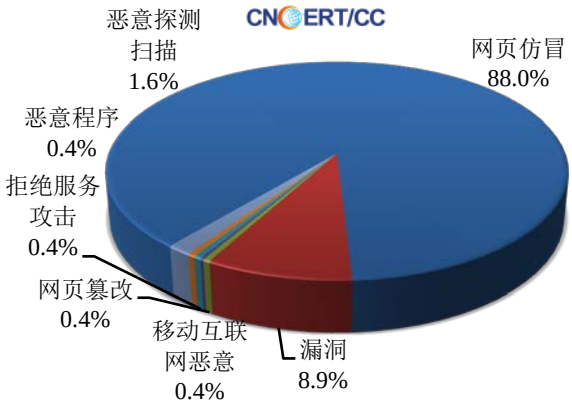
http://www.cnvd.org.cn/webinfo/list?type=4

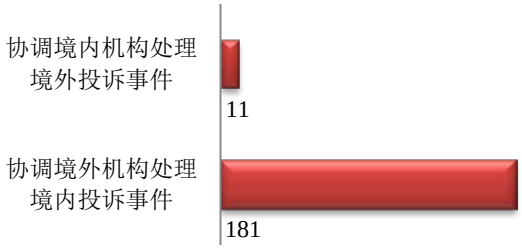
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 450 起，其中跨境网络安全事件 192 起。

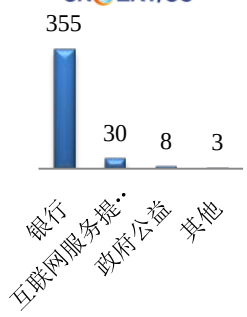
本周CNCERT处理的事件数量按类型分布
(10/15-10/21)



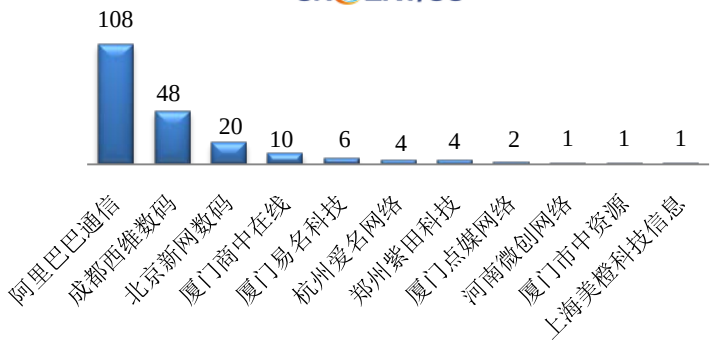


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 396 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 355 起和互联网服务提供商仿冒事件 30 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (10/15-10/21)

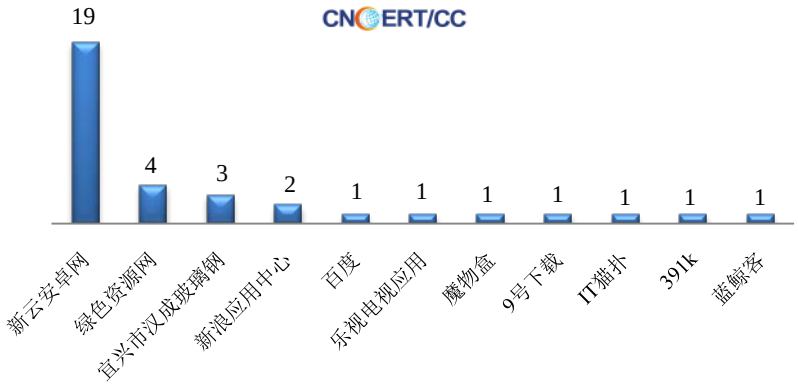


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (10/15-10/21)



本周，CNCERT 协调 11 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 35 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 (10/15-10/21)



业界新闻速递

1、澳门立法会全体会议一般性通过《网络安全法》法案

中新网 10 月 19 日消息 2018 年 10 月 18 日，澳门立法会全体会议一般性通过《网络安全法》法案。澳门保安司司长黄少泽引介时表示，《网络安全法》能够为构建澳门网络安全体系提供法律依据，同时将关乎澳门社会正常运作的基础建设，定义为“关键基础设施”，明确设施的营运者和社会各相关方面就网络安全应该负有的义务和责任，并在行政管理层面上落实各项网络安全工作，包括注视异常状况、风险评估、预警、防范、监管，以及其他应对工作等，从而构建一个有效的网络安全防范管理体系，提升澳门防范和应对网络安全的能力，以更好维

护国家总体安全和澳门本地社会公共安全，实现《澳门特别行政区五年发展规划(2016-2020)》有关建设“智慧城市”和“安全城市”的发展目标。

2、美情报和国家安全联盟发布“网络指标和警告框架”白皮书

安全内参 10 月 17 日消息 综合美国智库情报和国家安全联盟网站及美国媒体 2018 年 10 月 17 日反映，应多个联邦机构的请求，美国智库情报和国家安全联盟（INSA）于 10 月 16 日发布“网络指标和警告（I&W）框架”白皮书，以便相关组织更好地分享关于网络攻击的迹象和警告，并将这些数据分解为可以监测的指标。该框架旨在为政府、学术界和行业专业人士提供一个实用的分析过程，在这个过程中，预期的攻击场景被分解为可持续监测的指标，并对实际的攻击发出警告。

3、印度设立三机构 应对网络太空及特种作战威胁

参考消息网 10 月 18 日消息 印度在应对新的当代威胁方面又迈出了一步，内阁安全委员会最近批准成立了 3 个机构：国防网络局、国防航天局和特种作战司令部。报道称，另一位官员证实，这 3 个机构都将是三军机构，这意味着其将从每个军种抽调人员，在参谋长委员会主席的指挥下工作。

4、来自美国 19 个州的 3500 万选民记录被曝正在暗网兜售

黑客视界 10 月 17 日消息 据外媒 ZDNet 报道，两家威胁情报公司于最近发现大约 3500 万美国选民的个人信息正在一个热门的暗网论坛上被兜售，共涉及到 19 个洲。报道称，发现这一行为的两家公司分别是 Anomali Labs 和 Intel 471。这两家公司均表示，他们已经对在售的数据进行了全面审查，并确定数据真实有效。研究人员表示，这些数据包含了选民的全名、电话号码、居住地址、投票历史以及其他与投票相关的详细信息。

5、冰岛史上最大网络攻击行动：黑客冒充警方欺诈民众

cnBeta.COM10 月 15 日消息 2018 年 10 月 6 日，黑客以所入侵的帐号注册了 www.logregian.is 网域名称，与冰岛警方的官网 www.logreglan.is 只差了一个字母，并在邮件中威胁使用者若不遵守规定可能会遭到逮捕，继之提供来自伪造网站的连结。当使用者造访假冒的警察网站时，会被要求输入社会安全码，输入之后，该站竟然能够验证使用者的身分，从而跳出使用者的姓名，还要求使用者输入邮件中所附的验证码以再次验明正身。冰岛警方已认定这是冰岛迄今所出现的最大的网络攻击行动，也已确认许多收件人都已沦为受害者，并根据电子邮件及网站所使用的文字，以及黑客所拥有的冰岛民众资料，相信它是由内贼所为。

6、苹果系统遭攻击 黑客索要 17.4 万美元比特币作为赎金

新浪财经 10 月 20 日消息 一名 21 岁的土耳其 IT 分析师通过黑客手段入侵了苹果(220.65, 1.34, 0.61%)公司的系统，并威胁如果不补偿他的话就把苹果公司 3.19 亿用户的详细信息卖出去。这位分析师同时也是垂直数字媒体 Vasinity 的创始人。近期的黑客攻击案件激增，这些案件中的受害者大多是加密货币交易所。然而从目前这种事态发展来看，似乎没有任何一种系统可以成为“安全地带”。警方早些时候曾警告称，黑客会通过勒索软件劫持某些用户电脑上的文件，然后要求这些用户支付赎金以换取他们的文件。此外，警方还警告用户不要付钱给那些勒索他们的黑客。由于目前大多数黑客都要求支付比特币作为赎金，这一趋势也成了加密货币社区非常关注的问题，因为这个趋势让加密货币处于不利位置。现在已经有人指控称，加密货币主要被犯罪分子用来进行犯罪活动了。

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： 余江浩

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158