国家互联网应急中心

网络安全信息与动态周报

2018 年第 47 期

11 月 19 日-11 月 25 日

CNCERT/CC

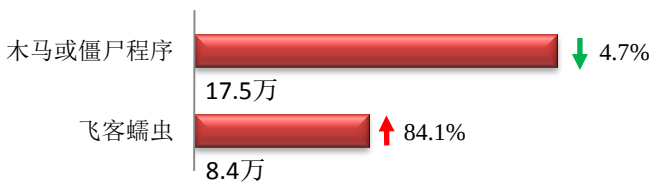
本周网络安全基本态势

境内感染网络病毒的主机数量	•26.0万	↑13.0%
境内被篡改网站总数 其中政府网站数量	•865 •39	↑61.1% ↑50.0%
境内被植入后门网站总数 其中政府网站数量	•573 •9	↓6.5% ↓35.7%
针对境内网站的仿冒页面数量	•1976	↑10.8%
新增信息安全漏洞数量 其中高危漏洞数量	•153 •61	↓24.3% ↓39.0%

=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

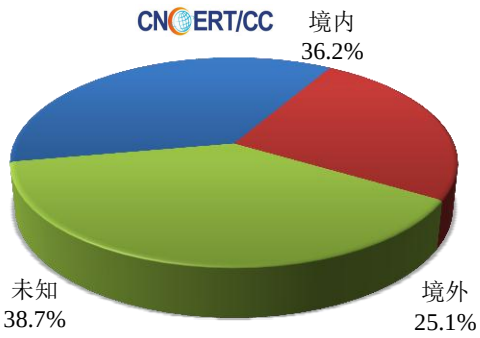
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 26.0 万个，其中包括境内被木马或被僵尸程序控制的主机约 17.5 万以及境内感染飞客（conficker）蠕虫的主机约 8.4 万。

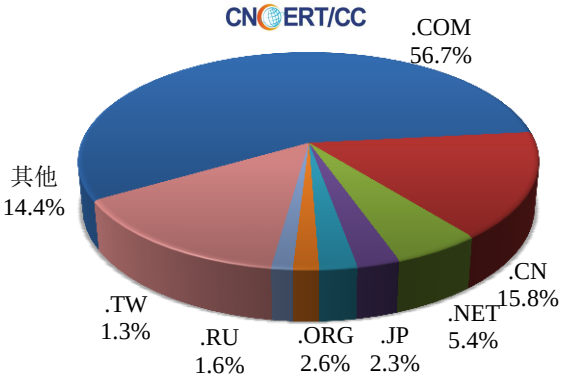


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 3735 个，涉及 IP 地址 5381 个。在 3735 个域名中，有 25.1%为境外注册，且顶级域为.com 的约占 56.7%；在 5381 个 IP 中，有约 51.6%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 546 个 IP。

本周放马站点域名注册所属境内外分布
(11/19-11/25)



本周放马站点域名所属顶级域的分布
(11/19-11/25)



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。

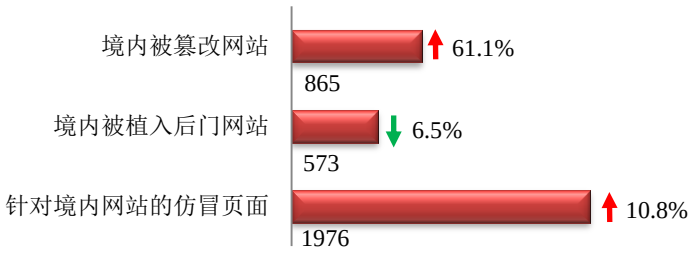
ANVA恶意地址黑名单发布地址

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。

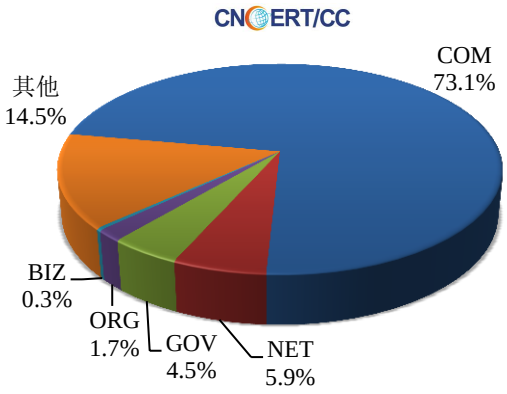
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 865 个；境内被植入后门的网站数量为 573 个；针对境内网站的仿冒页面数量为 1976 个。

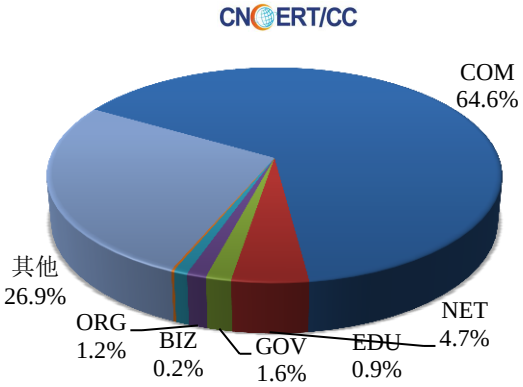


本周境内被篡改政府网站（GOV 类）数量为 39 个（约占境内 4.5%），较上周环比上升了 50.0%；境内被植入后门的政府网站（GOV 类）数量为 9 个（约占境内 1.6%），较上周环比下降了 35.7%；针对境内网站的仿冒页面涉及域名 525 个，IP 地址 259 个，平均每个 IP 地址承载了约 8 个仿冒页面。

本周我国境内被篡改网站按类型分布
(11/19-11/25)

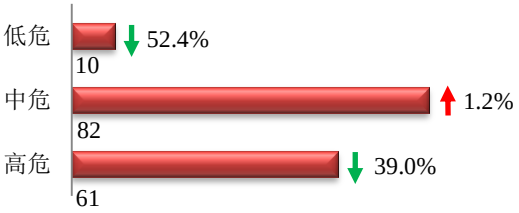


本周我国境内被植入后门网站按类型分布
(11/19-11/25)

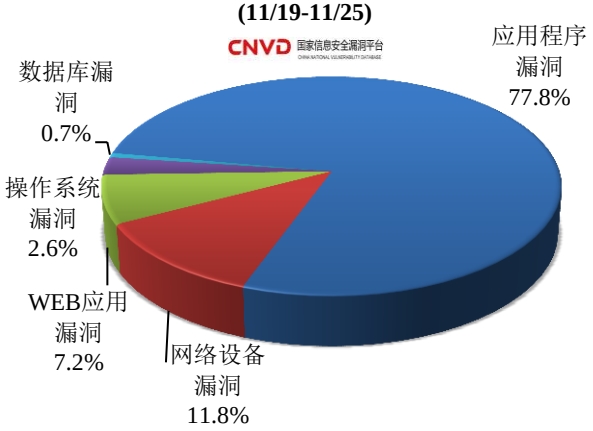


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 153 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
(11/19-11/25)



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

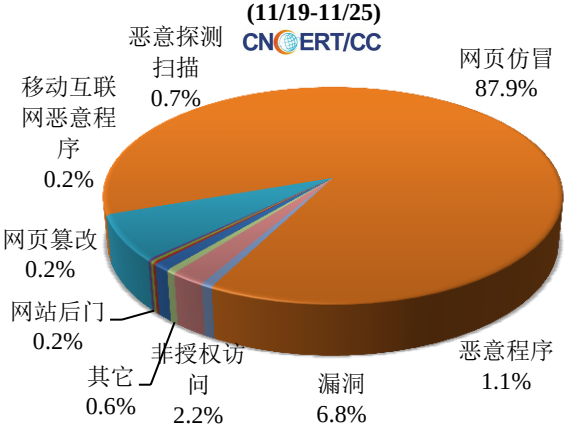
http://www.cnvd.org.cn/webinfo/list?type=4

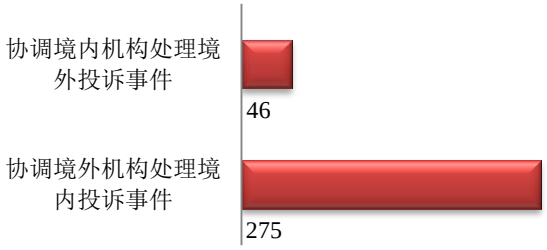
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 829 起，其中跨境网络安全事件 321 起。

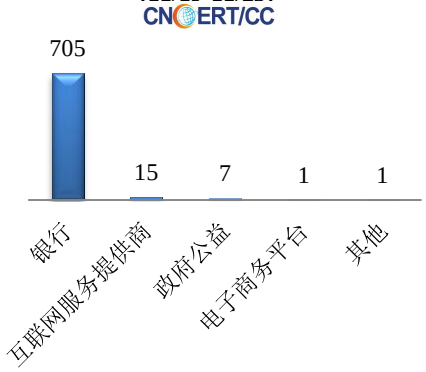
本周CNCERT处理的事件数量按类型分布 (11/19-11/25)



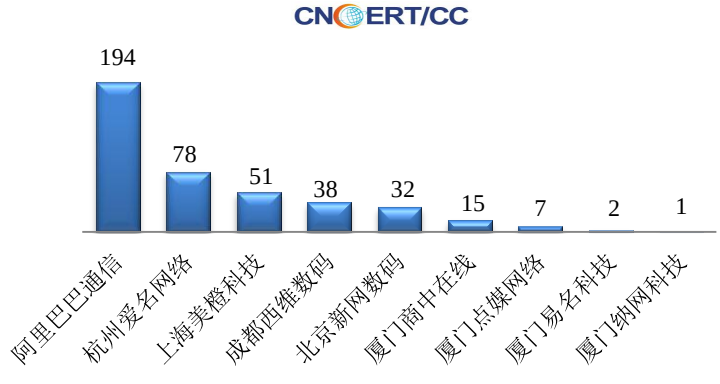


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 729 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 705 起和互联网服务提供商仿冒事件 15 起。

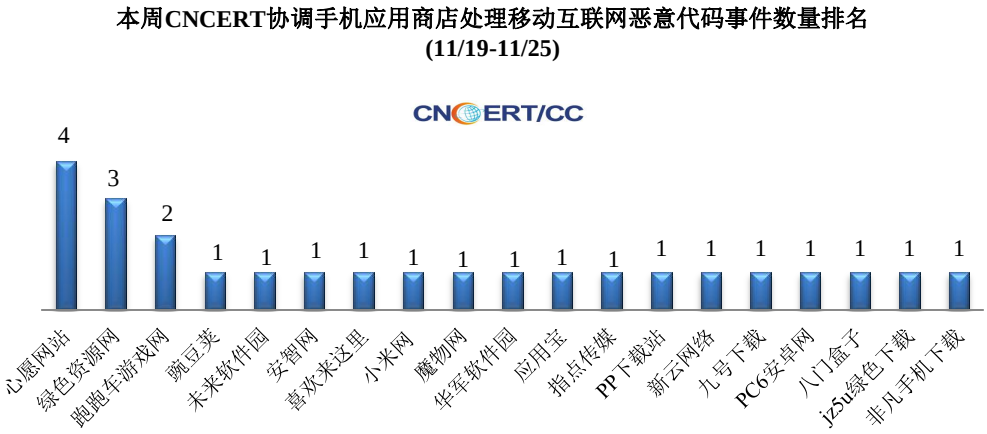
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (11/19-11/25)



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 (11/19-11/25)



本周，CNCERT 协调 19 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 25 个。



业界新闻速递

1、新加坡与加拿大、美国就网络安全问题展开合作

E 安全 11 月 20 日消息 据报道，新加坡政府已与两国签署伙伴关系协定，该协定内容涵盖数据共享、联合技术认证项目以及能力建设项目提案。新加坡已与加拿大、美国签署伙伴关系协定，该协定内容涵盖数据共享、联合技术认证计划以及能力建设举措。新加坡网络安全局（简称 CSA）表示，其与加拿大外交、贸易与发展部签订了为期两年的谅解备忘录（简称 MoU），其中包括在网络威胁与网络攻击上的信息交流、人力资源发展的最佳实践及其他各领域的合作。该伙伴关系包括提供技术与认证服务、网络安全发展标准以及区域网络安全能力建设。新加坡政府还同澳大利亚、法国与印度等国签署了现行的网络安全伙伴关系协定。

2、美国邮政服务 USPS 站点紧急修复安全漏洞：能够查看任何其它用户的详情

cnBeta.COM11 月 23 日消息 据外媒报道，赶在假期购物旺季之前，美国邮政服务 USPS 网站修正了一个安全漏洞，所有 USPS 网站注册用户（近 6000 万人）都能够利用该漏洞看到任何网站用户的个人详细信息。知名信息安全专家/调查记者 Brian Krebs 在本周三发文指出了此漏洞，他指出他在上周被一位不具名的安全研究者好友联系，利用的正是这一漏洞。这位信息安全研究者最早在一年前就发现并且尝试此漏洞，但从未得到一个正式的回复。当 Krebs 收到后就确认了研究者的发现，并且报告给 USPS。这一漏洞能够让任何已登录的 USPS 网站用户能够“向系统请求任何其它账号的账号详情”，利用了该网站验证机制 API 的通知递送服务 Informed

Visibility 缺陷，Krebs 声称其能够查看到邮箱地址、用户名、用户 ID 信息、街道住址、电话号码等信息。

3、英国议会遭受网络攻击 报告批评官方未做好应急准备

cnBeta.COM11 月 24 日消息 针对英国议会在 2017 年 6 月遭受网络攻击一事，前外交大臣玛格丽特·贝克特（Margaret Beckett）在其带领的一份委员会报告中批评称，官方未能在此前做好应急准备。正如卫报在去年的报道中提到的那样，约有 90 位议会官员的电子邮件账户使用了弱密码，导致被不法分子轻松侵入。最后，报告提醒政府应该意识到网络安全战略的必要性，敦促任命一位内阁级部长，由其负责整个国家级关键基础设施的网络安全与实施。

4、网络犯罪组织 Lazarus 植入后门攻击拉丁美洲金融机构

黑客视界 11 月 24 日消息 趋势科技发现，曾经攻击过亚洲和拉丁美洲金融机构的网络犯罪组织 Lazarus 分支 Bluenoroff 最近似乎再度活跃，他们近期的一系列活动展示了其攻击工具和技术的演变，上周他们从亚洲和非洲的 ATM 机中非法窃取了数百万美元。此外，研究人员还观察到他们成功将后门（趋势科技检测为 BKDR_BINLODR.ZNFJ-A）植入了拉丁美洲几家金融机构。研究人员经过跟踪分析后，根据加载器组件的服务创建时间确定，目标设备被安装后门的具体时间为 2018 年 9 月 19 日。这种攻击技术与 BAE Systems 分析的 2017 年 Lazarus 攻击与亚洲目标有相似之处。FileTokenBroker.dll 的使用是 2017 年该组织攻击的关键部分，他们似乎也在最近的事件中使用了相同的模块化后门。

5、俄罗斯黑客工具“Cannon”正在美欧计算机上进行更隐蔽的攻击

E 安全 11 月 21 日消息 网络安全专家表示，俄罗斯黑客拥有一种新工具，可以在不被察觉的情况下访问敏感计算机。而且他们正在利用它来瞄准美国和欧洲政府实体，以及苏联的前领土。网络安全公司 Palo Alto Networks 在周二的博客文章中描述了黑客工具，它称之为“Cannon”。Cannon 是一种恶意软件，黑客潜入目标计算机并用于截取受感染计算机主页的屏幕截图。然后，该软件使用电子邮件将图像发送回黑客并接收新指令。它就像是计算机上的间谍相机，可以将图像发送回家，显然是送到俄罗斯。在其他两家网络安全公司告诉路透社，俄罗斯黑客冒充美国国务院的员工向智囊团，企业和政府机构发送网络钓鱼电子邮件之后不到一周，Palo Alto Networks 就发现了这个名为 Cannon 的黑客工具，但是他们没有透露黑客在攻击活动中扮演的角色，也没有提供有关特定目标国家的更多信息。

6、最大暗网服务商遭受攻击导致 6500 个网站瘫痪

黑客视界 11 月 20 日消息 暗网托管服务商允许任何人在不泄露其身份的情况下托管网站，而且他们的客户则有参与非法活动的可能。暗网未被编入索引，因此从 Google 和 Bing 等常规搜索引擎无法进入这些网站。尽管如此，某些搜索引擎存在于暗网世界中，但想要找到它们的人不是非法活动者，就是执法机构人员。除了搜索引擎之外，即使是常规浏览器（如 chrome 和

explorer）也难以到达暗网世界。要访问这些站点，需要通过名为 Tor 的浏览器。目前暗网托管服务仍然存在，暗网世界也一团混乱。毒贩、勒索者、非法军火商和其他可疑方使用暗网托管服务的情况并不少见，所以执法机构被波及也实属正常。根据 Daniel 的托管业务模式，这些 6,500 个网站中的所有数据都将彻底丢失，因为它们没有维护任何备份。与此同时，Daniel 的发言人 Daniel Winzen 证实了这一消息，并表示事件发生在 2018 年 11 月 15 日晚上 10 点到 11 点之间。他仍在寻找漏洞，恢复服务的过程中。

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：丁丽

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158