国家互联网应急中心

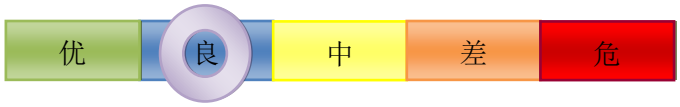
网络安全信息与动态周报

2017 年第 41 期

10 月 2 日-10 月 8 日

CNCERT/CC

本周网络安全基本态势

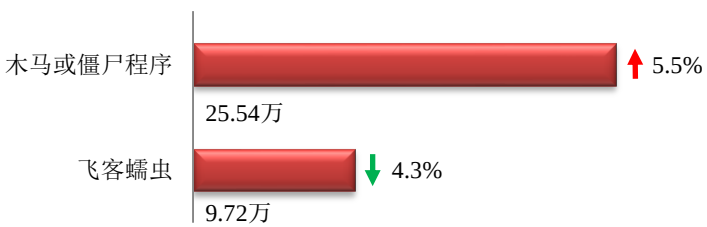


境内感染网络病毒的主机数量	•35.26万	↑ 2.6%
境内被篡改网站总数 其中政府网站数量	•2,753 •44	↑ 74.7% ↑ 51.7%
境内被植入后门网站总数 其中政府网站数量	•765 •34	↓ 30.1% ↓ 42.4%
针对境内网站的仿冒页面数量	•251	↓ 11.0%
新增信息安全漏洞数量 其中高危漏洞数量	•328 •119	

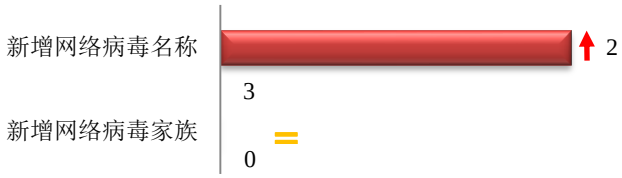
═表示数量与上周相同　↑表示数量较上周环比增加　↓表示数量较上周环比减少

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 35.26 万个，其中包括境内被木马或被僵尸程序控制的主机约 25.54 万以及境内感染飞客（conficker）蠕虫的主机约 9.72 万。

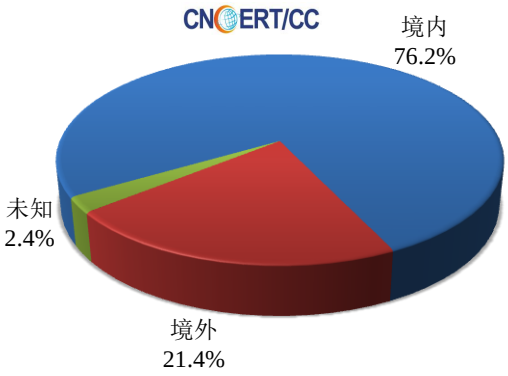


本周 CNCERT 捕获的新增网络病毒文件，按网络病毒名称统计新增 3 个，按网络病毒家族统计无新增。

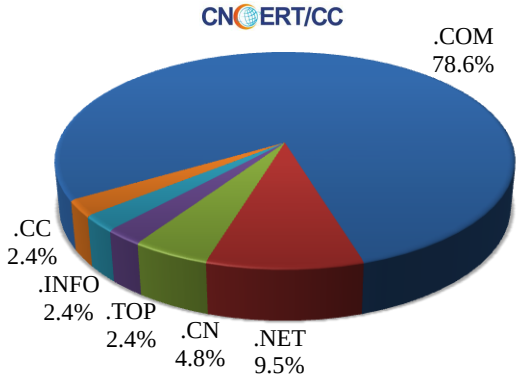


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 42 个，涉及 IP 地址 268 个。在 42 个域名中，有 21.4%为境外注册，且顶级域为.com 的约占 78.6%；在 268 个 IP 中，有约 8.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 2 个 IP。

本周放马站点域名注册所属境内外分布
(10/2-10/8)



本周放马站点域名所属顶级域的分布
(10/2-10/8)



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。

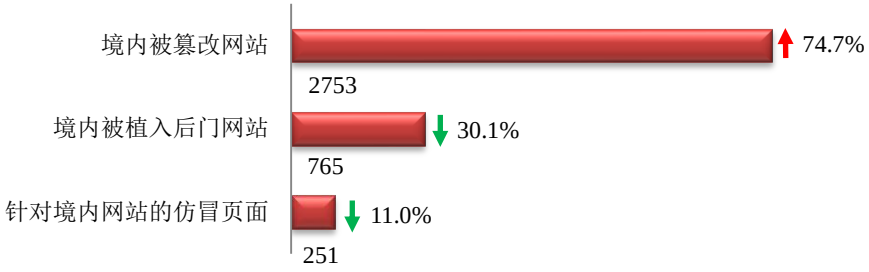
ANVA恶意地址黑名单发布地址

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。

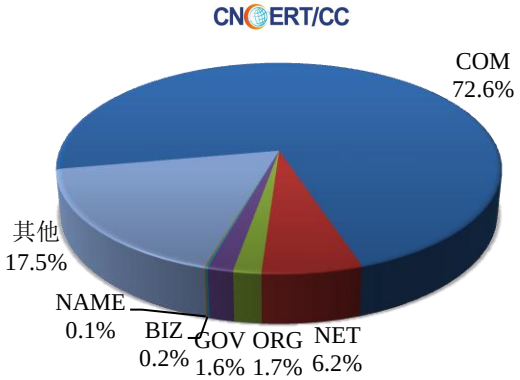
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2753 个；境内被植入后门的网站数量为 765 个；针对境内网站的仿冒页面数量为 251。

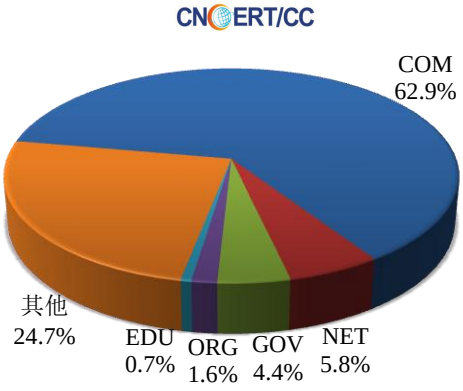


本周境内被篡改政府网站（GOV 类）数量为 44 个（约占境内 1.6%），较上周环比上升了 51.7%；境内被植入后门的政府网站（GOV 类）数量为 34 个（约占境内 4.4%），较上周环比下降了 42.4%；针对境内网站的仿冒页面涉及域名 202 个，IP 地址 107 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(10/2-10/8)

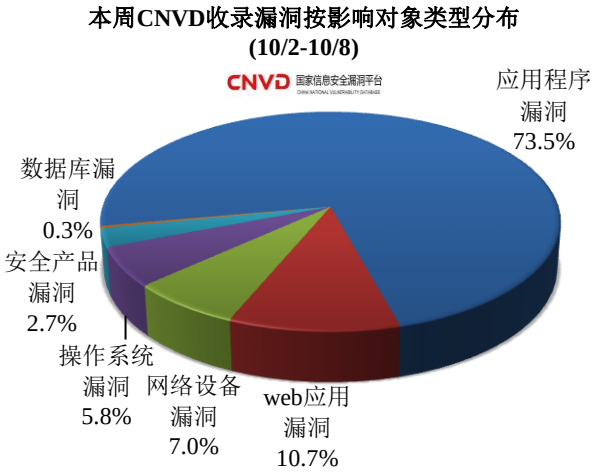


本周我国境内被植入后门网站按类型分布
(10/2-10/8)



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 328 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。

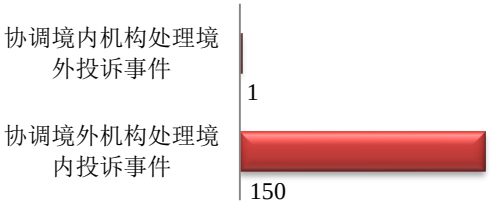
CNVD漏洞周报发布地址

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。

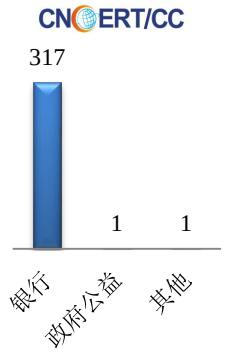
本周事件处理情况

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 319 起，其中跨境网络安全事件 151 起。

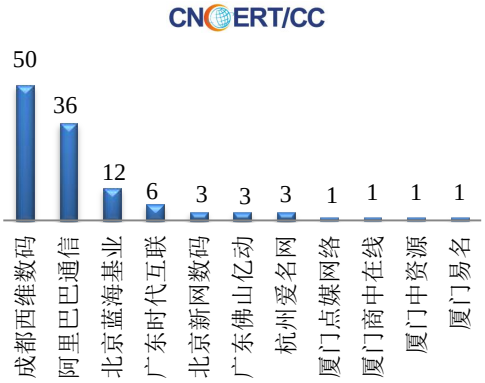


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 319 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 317 起和政府公益仿冒事件 1 起。

本周CNCERT处理网页仿冒事件数量
按仿冒对象涉及行业统计(10/2-10/8)



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 (10/2-10/8)



业界新闻速递

1、美国立法者想限制国安局针对美国人的网络监控

cnBeta.COM10 月 5 日消息 据路透社报道，一个由立法议员组成的团体周三公布了一项法案，将详细调查美国国家安全局（NSA）无保证的互联网监督计划的各方面，努力为美国公民提供额外的隐私保护措施。这个法案将在当地时间正式推出。由众议院司法委员会撰写的法案被公民自由团体视为国会改革“外国情报监察法（FISA）”第 702 条款的最佳机会。“外国情报监察法（FISA）”第 702 条款允许美国情报机构窃取和存储来自美国境外的外国嫌疑犯的大量数字通信信息。但是，该计划的分类细节在 2013 年遭举报人爱德华·斯诺登（Edward Snowden）揭露，称美国国家安全局（NSA）大规模搜集个人信息等。然后，美国联邦调查局可以在没有搜查令的情况下对这些通信进行搜索。据路透社透露，该法案的一个讨论稿部分限制了美国联邦调查局根据第 702 条款收集美国公民数据的能力，要求该机构在寻找犯罪证据时获得搜查令。FISA 法案将于 2017 年 12 月 31 日过期。如果新的修正案获得通过，将被授权有 6 年的有效期，这意味着美国国家安全局可能在 2023 年可能恢复活动。

2、英国电信与国际刑警组织 IGCI 签署数据共享协议

HackerNews.cc10 月 8 日消息 英国电信近期发表声明，宣称已经与新加坡国际刑警组织 IGCI 签署数据共享协议，旨在促进全球网络安全合作，保护家庭、消费者、企业和政府免遭犯罪攻击。据悉，该协议为网络威胁交流提供了一个标准框架，主要关注并分析网络空间、新兴与已知的网络威胁，以及网络犯罪分子恶意攻击的影响趋势。英国电信的威胁情报专家透露，他们将为 IGCI 提供不断变化的全球威胁形势与见解，旨在帮助国际刑警组织查明犯罪行动并快速采取措施打击网络犯罪。IGCI 执行董事 Noboru Nakatani 表示：“当今网络威胁态势的规模与复杂程度让我们深刻认识到，如果想要有效地打击这种全球现象，就必须与全球各部门加强合作。

所以，国际刑警组织与英国电信签署的共享协议是我们确保执法机构快速应对网络威胁的重要一步。”

3、雅虎 30 亿帐号或全部受早先数据泄露事件影响

新浪网 10 月 4 日消息 北京时间 4 日早间 CNBC 称，雅虎周二表示，所有雅虎帐号在 2013 年 8 月的一次大规模数据泄露事件中都曾受到影响。雅虎去年披露，超过 10 亿个帐号在那次网络攻击中受到影响。但该公司周二表示，所有帐户都有可能受到了影响。该公司在其账号安全更新页面最近的一次更新中披露了这一发现，称通过与威瑞森通信公司（Verizon Communications）的业务合并过程中获得的新情报证实，此次网络攻击的影响范围远超过此前的估计。雅虎表示，将开始向此前没有被通知此次攻击的帐号发出提醒，要求他们更改密码，以防止信息泄露。

4、国外著名评论网站 Disqus 被黑，逾 1750 万用户信息在线泄露

HackerNews.cc10 月 8 日消息 据外媒报道，国外著名的第三方评论管理网站 Disqus 近期发表声明，证实公司已于 2012 年被黑且泄露超过 1750 万条个人邮箱地址。然而，这些已泄露的邮箱账户中大约有 1/3 的账户包含密码，一些泄露的账户甚至可以追溯至 2007 年，另外许多 Disqus 账户没有密码，因为他们使用第三方账号（如 FB 和 Google 账号）注册评论服务。尽管早在 2012 年信息就被泄露，但是 Disqus 本周才发现用户信息被黑，作为安全措施，Disqus 将提醒密码被泄露的用户修改密码。实际上国内用户也经常会收到一些（很长时间未登录的）国外网站修改密码的邮件，一般情况下这也是许多网站账户信息遭到泄露时的补救措施。据悉，Disqus 在了解到信息泄露的 24 小时之内，设法评估损失、确定时间表、重置泄露用户密码，及时公告并与新闻界坦诚相待。

5、黑客伪造美国合法金融机构的安全信息发动网络钓鱼攻击

HackerNews.cc10 月 2 日消息 据外媒 9 月 29 日报道，安全研究人员近期发现网络犯罪分子通过伪造来自美国银行与 TD 商业银行等私人金融机构的合法域名、机构标志与其邮件底部的保密声明发送网络钓鱼邮件，旨在向不知情受害者分发恶意软件、窃取重要信息。调查显示，攻击者伪造合法银行安全信息发送网络钓鱼邮件，并在邮件中指示用户下载附件、填写个人信息并对其进行回复等一系列操作。据悉，该封电子邮件中所附带的 Word 文档包含一款恶意软件，用户一旦下载并安装将会允许攻击者在 Windows 设备上重写用户目录文件。值得注意的是，该款恶意软件可以规避部分杀毒软件检测，因为附带恶意软件的文档是安全的。若受害者设备成功安装该款恶意软件，攻击者就可对其进行访问与操控，从而窃取用户重要信息。

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。截止 2016 年，CNCERT 与 69 个国家和地区的 185 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：周彧

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158