国家互联网应急中心

网络安全信息与动态周报

2019 年第 40 期

9 月 30 日-10 月 6 日

CNCERT/CC

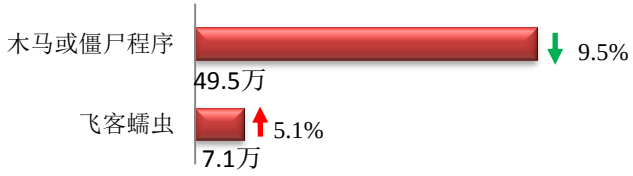
本周网络安全基本态势

境内感染网络病毒的主机数量	•56.6 万	7.9%
境内被植入后门网站总数 其中政府网站数量	•2863 •8	16.3% 75.8%
针对境内网站的仿冒页面数量	•35	35.2%
新增信息安全漏洞数量 其中高危漏洞数量	•0 •0	100.0% 100.0%

═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

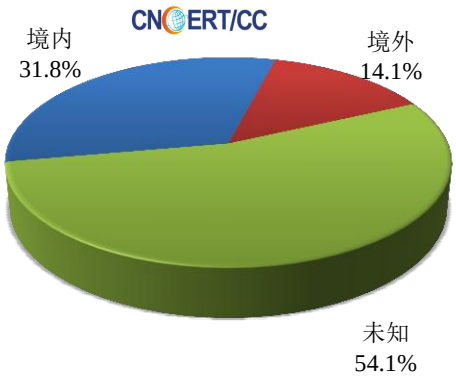
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 56.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 49.5 万以及境内感染飞客（conficker）蠕虫的主机约 7.1 万。

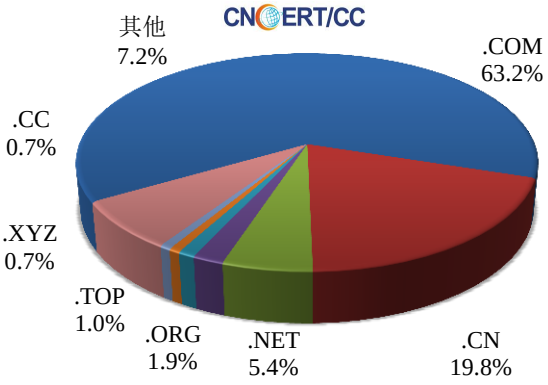


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 1159 个，涉及 IP 地 2188 个。在 1159 个域名中，有 14.1%为境外注册，且顶级域为.com 的约占 63.2%；在 2188 个 IP 中，有约 25.1%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 244 个 IP。

本周放马站点域名注册所属境内外分布
(9/30-10/6)



本周放马站点域名所属顶级域的分布
(9/30-10/6)



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。

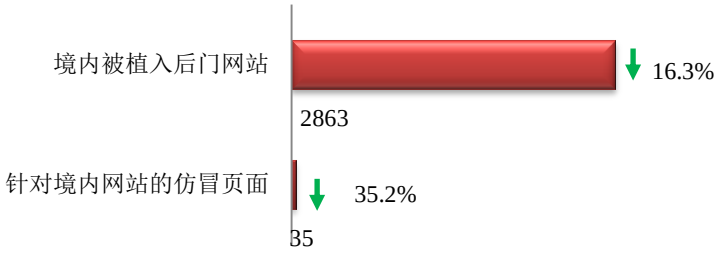
ANVA恶意地址黑名单发布地址

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。

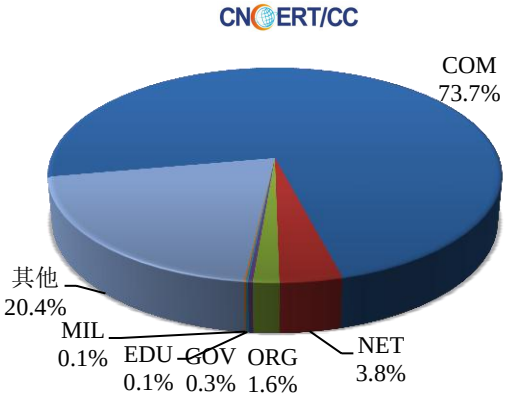
本周网站安全情况

本周 CNCERT 监测发现境内被植入后门的网站数量为 2863 个；针对境内网站的仿冒页面数量 35 个。



本周境内境内被植入后门的政府网站（GOV 类）数量为 8 个（约占境内 0.3%），较上周环比下降 75.8%；针对境内网站的仿冒页面涉及域名 22 个，IP 地址 18 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被植入后门网站按类型分布
(9/30-10/6)



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 0 个，信息安全漏洞威胁整体评价级别为中。

低危	0
中危	0
高危	0

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

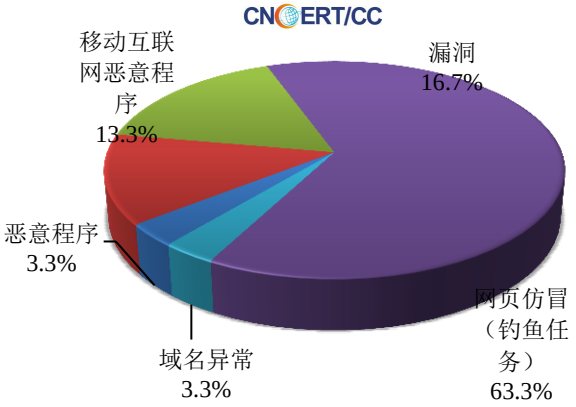
http://www.cnvd.org.cn/webinfo/list?type=4

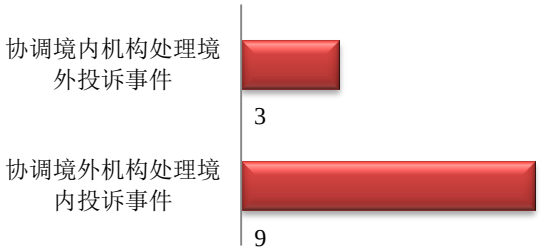
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 30 起，其中跨境网络安全事件 12 起。

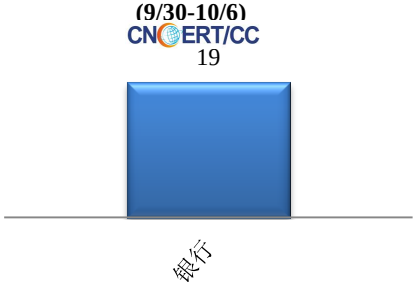
本周CNCERT处理的事件数量按类型分布 (9/30-10/6)



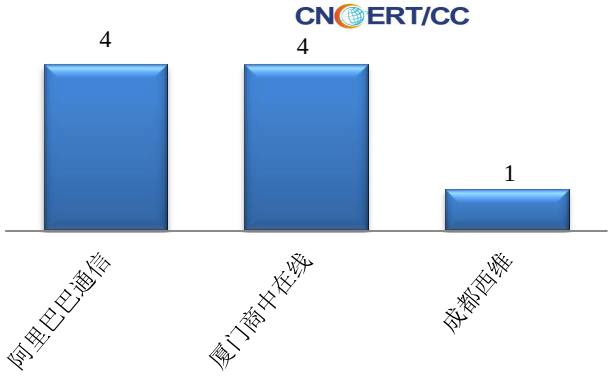


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 19 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 19 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (9/30-10/6)

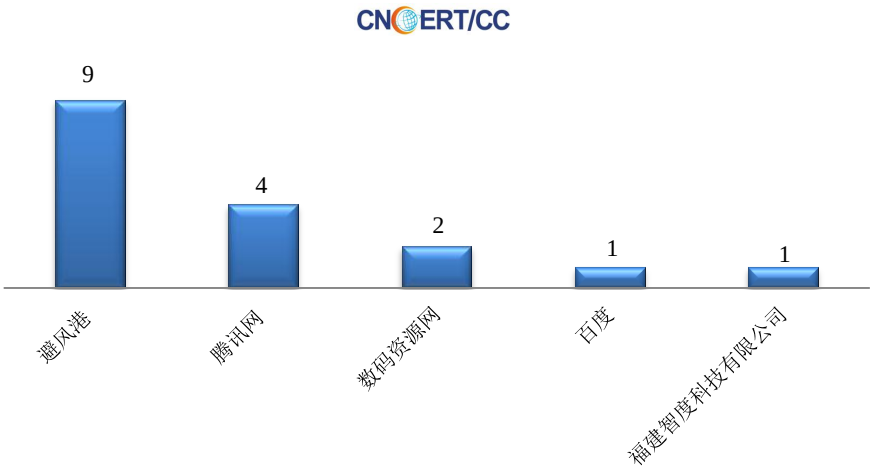


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (9/30-10/6)



本周，CNCERT 协调 5 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 17 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
(9/30-10/6)



业界新闻速递

1、《儿童个人信息网络保护规定》10 月 1 日正式实施

10 月 1 日人民网消息，由国家互联网信息办公室发布的《儿童个人信息网络保护规定》于 10 月 1 日正式实施。据专家介绍，这是我国第一部专门针对儿童网络保护的立法，明确了任何组织和个人不得制作、发布、传播侵害儿童个人信息安全的信息，确定了儿童个人信息网络保护的具体原则，以及网信部门和其他有关部门的监管职责。该规定填补了互联网时代儿童个人信息保护的法律空白。

2、英国上诉法院允许就谷歌非法收集 iPhone 用户数据提起集体诉讼

10 月 2 日《金融时报》消息,针对谷歌从 400 多万 iPhone 用户那里收集数据，伦敦上诉法院允许对谷歌的这一行为提起诉讼。这推翻了 2018 年的一项法律裁决，那次的裁决实际上阻止了针对谷歌这一行为采取任何法律行为的途径。

原告表示，Alphabet 旗下的谷歌 2011 年 6 月至 2012 年 2 月期间，绕过 Safari 浏览器上的隐私设置，非法访问了苹果 iPhone 用户的互联网浏览数据。苹果 Safari 浏览器中的安全设置旨在阻止用于打造针对性广告的第三方跟踪 Cookie。之前在收集了 iPhone 用户的浏览习惯数据后，谷歌据称已经确定了用户的性别、种族、民族、财务细节和其他信息，然后将个人归类到“足球爱好者”等各种标签下，并向广告商提供访问权限。

谷歌表示，保护用户的隐私和安全一直是谷歌的首要任务。不过，“这起案件与近十年前发生的事情有关，当时我们已经处理了这些事件。”谷歌一位女发言人说，“我们认为这是没有价值的，应该被驳回。”

3、Whatsapp 被曝漏洞 一张 GIF 动图黑客便可接管账户

10 月 3 日 TNW 消息,Facebook 旗下即时通讯工具 WhatsApp 修复了一个安全漏洞，此前通过该漏洞，黑客可以用恶意 GIF 动图入侵该软件。当用户在他们的图库中打开一个恶意 GIF 动图时，就可能触发黑客攻击。GIF 被打开后，Whatsapp 软件里面的内容可能会被盗用，包括用户个人信息、聊天记录等。

据悉，手机系统为 Android 8.1 和 Android 9 的设备容易遭受此类攻击。一位名叫沃克的研究人员发现了这一漏洞，并于上周在博客上发表了相关文章。Facebook 旗下的 WhatsApp 上个月发布了一个补丁，不过但 WhatsApp 的一位发言人称，很少有用户收到该类攻击，团队将致力于保障用户安全。

4、英美达成数据跨境获取执法协议 美国《云法案》首现域外突破

10 月 3 日美国司法部官网消息，美国政府与英国政府首次正式就执法部门电子数据的跨境获取达成协议，美国“云法案”（CLOUD ACT，也即《澄清合法使用海外数据法案》）取得历史性海外推进，将对数据治理国际格局产生重大影响。

在恐怖主义犯罪、儿童色情和其他网络犯罪的情形下，两国执法部门皆可在授权下，并在数据保护法的限制范围内——特别是在牵涉美国的死刑案件和英国的言论自由案件时——直接向有关科技公司，而非通过当地政府，采集数据。而在本协议签署之前，根据既有的两国法律互助协定，这一采集程序可能需要花长达两年的时间完成，并可能导致大量数据因不能及时采集而灭失。

美国司法部长威廉·巴尔认为，这一协议可以通过提供快速有效的数据获取手段，加强英美两国在共同打击上述严重犯罪中的合作，共同应对 21 世纪的新挑战、新威胁，并在为两国公民提供更佳的安全保证的同时，保护两国公民的隐私和自由。

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：杨凯

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315