国家互联网应急中心

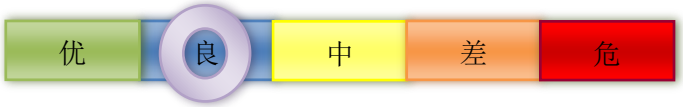
网络安全信息与动态周报

2018 年第 37 期

9 月 10 日-9 月 16 日

CNCERT/CC

本周网络安全基本态势

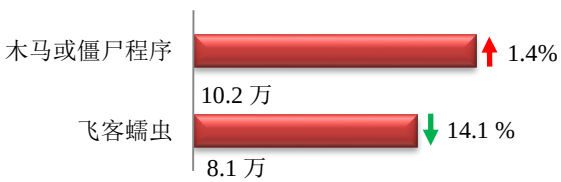


境内感染网络病毒的主机数量	•18.2万	6.1%
境内被篡改网站总数 其中政府网站数量	•575 •33	4.3% 19.5%
境内被植入后门网站总数 其中政府网站数量	•627 •17	17.0% 26.1%
针对境内网站的仿冒页面数量	•2885	63.6%
新增信息安全漏洞数量 其中高危漏洞数量	•301 •117	29.0% 33.9%

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*

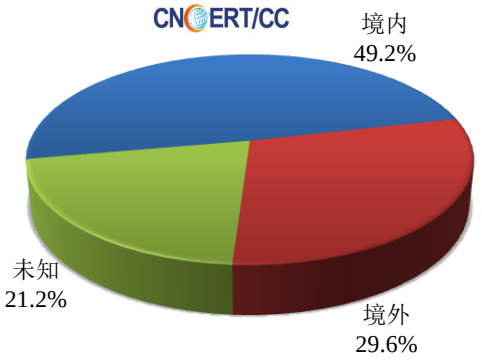
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 18.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 10.2 万以及境内感染飞客（conficker）蠕虫的主机约 8.1 万。

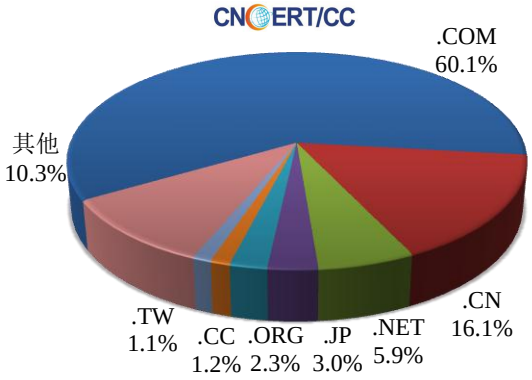


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 3163 个，涉及 IP 地址 78642 个。在 3163 个域名中，有 29.6%为境外注册，且顶级域为.com 的约占 60.1%；在 78642 个 IP 中，有约 34.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 369 个 IP。

本周放马站点域名注册所属境内外分布
(9/10-9/16)



本周放马站点域名所属顶级域的分布
(9/10-9/16)



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。

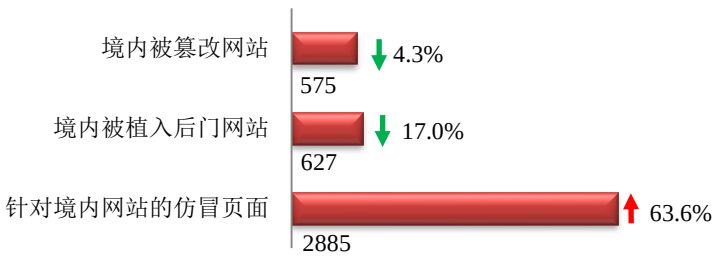
ANVA恶意地址黑名单发布地址

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。

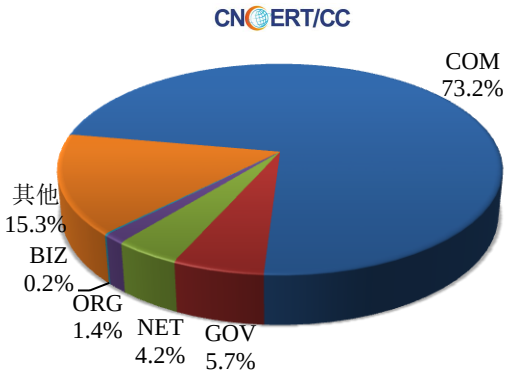
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 575 个；境内被植入后门的网站数量为 627 个；针对境内网站的仿冒页面数量为 2885。

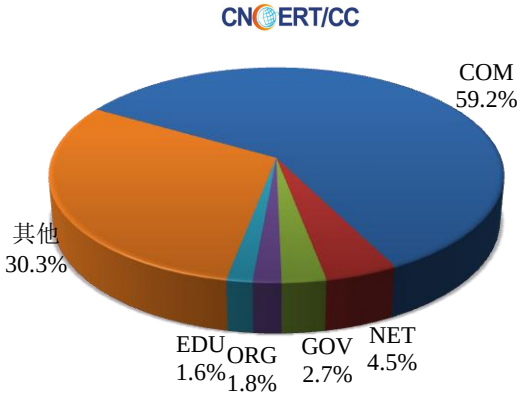


本周境内被篡改政府网站（GOV 类）数量为 33 个（约占境内 5.7%），较上周环比下降了 19.5%；境内被植入后门的政府网站（GOV 类）数量为 17 个（约占境内 3.0%），较上周环比下降了 26.1%；针对境内网站的仿冒页面涉及域名 1089 个，IP 地址 383 个，平均每个 IP 地址承载了约 8 个仿冒页面。

本周我国境内被篡改网站按类型分布
(9/10-9/16)

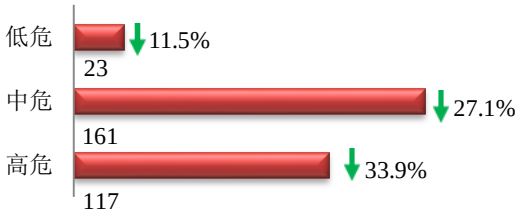


本周我国境内被植入后门网站按类型分布
(9/10-9/16)

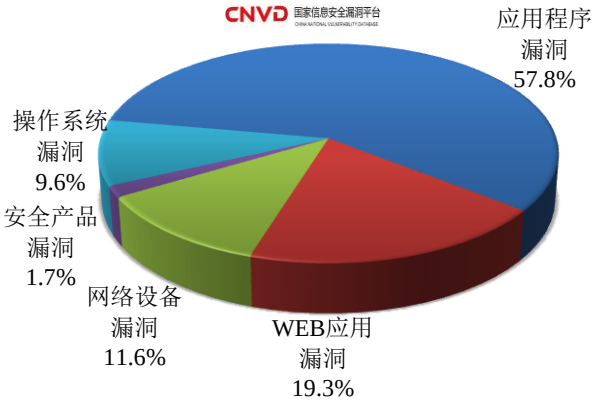


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 301 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
(9/10-9/16)



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

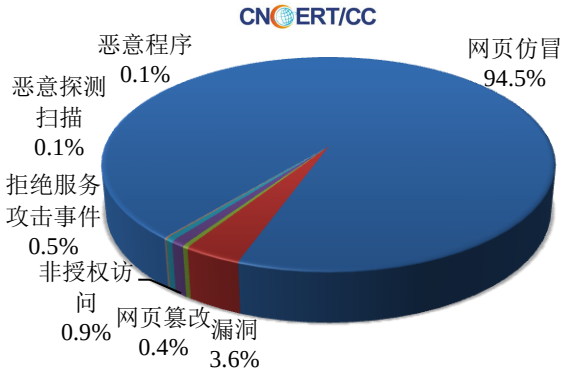
http://www.cnvd.org.cn/webinfo/list?type=4

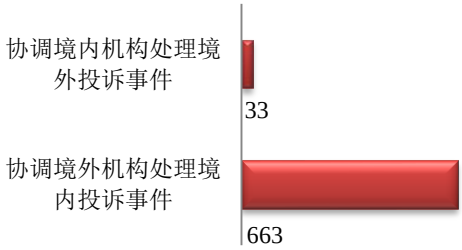
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 1358 起，其中跨境网络安全事件 696 起。

本周CNCERT处理的事件数量按类型分布 (9/10-9/16)

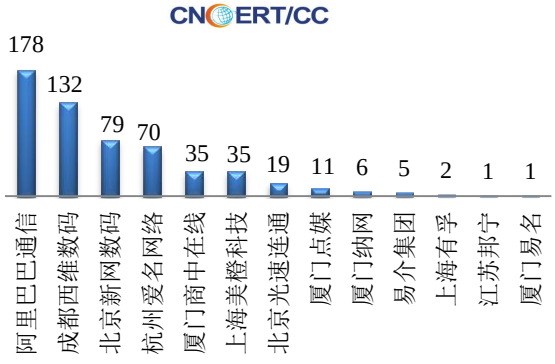




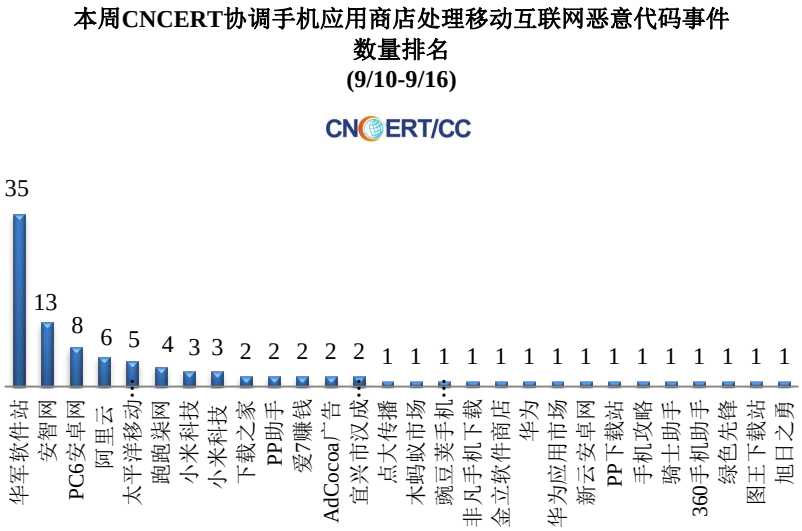
本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1276 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 1276 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(9/10-9/16)

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 (9/10-9/16)



本周，CNCERT 协调 28 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 102 个。



业界新闻速递

1.中国互联网安全标准被国际接纳 取得重大进展

cnBate 9 月 12 日消息，互联网域名系统北京市工程研究中心(简称域名工程中心，英文缩写 ZDNS)在中国科学院软件园宣布，由中国技术人员牵头起草的互联网安全标准正式被国际社会接纳，成为互联网国际技术标准 IETF RFC8416。会上还发布了自主开发的域名系统基础软件“红枫”系统、全球运行速度最快的域名服务器，以及首台国产化域名服务器。这是我国互联网社区为国际互联网技术发展作出的又一贡献。

随着互联网的广泛应用，互联网自身的安全问题也日益突显出来。为解决互联网上虚假地址引发的的“安全漏洞”问题，全球互联网技术标准制定组织 IETF 自 2012 年开始发布了一系列 RPKI(资源公共密钥基础架构)技术标准，通过让 IP 地址进行验证的方式来解决互联网上“伪基站”问题。这是互联网自诞生以来至关重要的一次安全升级，也给互联网治理机制的调整带来了新的机遇。RFC8416 是 IETF 刚发布的最新一个 RPKI 国际标准，也是 RPKI 标准起草组(SIDR WG)产出的最后一个标准，RFC8416 实现了对 RPKI 这一认证机制的本地自主可控。

会上发布了由域名工程中心完全自主开发的互联网基础软件“红枫”(Maple DNS)。中国互联网发展迅速，应用的深度和广度都走在世界前列，传统的域名服务软件已经不能适应中国市场需求。红枫软件是域名工程中心花了 8 年时间打磨出来一套高性能、智能化的基础软件，达到了国际领先水平。

基于红枫软件，域名工程中心和中科曙光联合推出首台国产化域名服务器。该服务器首次实现了域名解析基础软件系统在国产芯片的实践落地，扩大了国产芯片的使用生态。

会上还发布了一款自主研发的高性能域名服务器。根据国际同行网站显示，该高性能服务器运行速度是国际同行最快服务器的 1.6 倍。单台高性能服务器可防护 10G 带宽流量。该服务器将有力应对针对域名系统的

DDoS 攻击，从而帮助运营商级别的机构大大提升网络安全保障能力。

除了互联网国际标准、高性能设备和红枫软件之外，本次会议期间，域名工程中心还发布了“ZDNS 域名云服务平台 2.0”、“ZDNS 企业网络基础设施 IPv6 升级解决方案”、“基于 k8s 平台的企业级云 DNS 解决方案”、“ZDNS 企业品牌顶级域名解决方案”、“ZDNS 域名系统维保服务体系升级版”等一系列产品和服务。

2.汤森路透发布针对中小企业的网络安全白皮书

E 安全 9 月 12 日讯 汤森路透发布白皮书，以帮助中小企业保护自身免受网络安全事件侵害。这份白皮书就中小企业如何制定强大的信息安全战略提供指导，其中包括运用预防、检测和反映性控制措施。白皮书指出，在当今的商业环境中，企业必须保护暴露在互联网和其他外部接口的每个系统。信息安全的任何弱点都可能使整个组织机构陷入危险境地，可能会造成业务中断、面临罚款和罚款，声誉受损等后果。白皮书还探讨了黑客攻击薄弱信息系统的方式和原因，并概述了企业应建立关键控制措施，以加强防御。

3.Mozilla 创始人投诉谷歌：违反 GDPR 法规 泄露用户数据

新浪科技讯 北京时间 9 月 13 日晚间消息，Mozilla 联合创始人布兰登·艾奇(Brendan Eich)创立的浏览器公司 Brave 今日在英国和爱尔兰对谷歌和其他广告公司进行了投诉，称这些公司泄露用户数据的行为违反了欧盟新生效的数据隐私法规《通用数据保护条例》(以下简称“GDPR”)。

GDPR 于今年 5 月正式生效。该法规旨在赋予欧盟居民对个人数据有更多的控制权。如果一家公司不遵守这项条例，将面临最高相当于其全球年度营业额 4%或 2000 万欧元(约合 2340 万美元)的罚款，

Brave 和其他一些原告称，谷歌和其他一些广告公司存在大规模、系统性的数据泄露行为。虽然 GDPR 在正式实施前，已经赋予企业两年的准备时间，但包括谷歌在内的广告科技公司至今仍未遵守该规定。

原告称，当用户访问网站时，谷歌和其他一些广告公司出于拍卖和投放广告的目的，将用户个人数据和访问记录发送到几十家、乃至上百家公司，而且是在用户不知情的情况下。毫无疑问，这违反了 GDPR 的规定。

对此，谷歌称，已与欧洲监管机构协商，实施了强有力的隐私保护措施，并已承诺遵守 GDPR。

4.布里斯托尔机场遭遇网络攻击，致航班信息仅能通过白板发布

英国广播公司（BBC）16 日报道，布里斯托尔机场在上周遭遇了一起基于勒索软件的网络攻击，导致机场电子显示屏被迫离线两天。在此期间，所有的航班信息仅能通过白板和记号笔发布。

BBC 的报道得到机场发言人 James Gore 的证实。James Gore 表示，由于布里斯托尔机场的电子显示屏控制系统遭到了勒索软件的感染，因此他们在上周五对电子显示屏进行了关闭处理。

另外，James Gore 还表示，机场方面并没有选择向攻击者妥协及支付赎金。

来自安全专家的观点认为，有迹象表明这起攻击并非专门针对布里斯托尔机场发起的，布里斯托尔机场很可能只是大规模勒索软件分发活动中的其中一名受害者。

好消息是，布里斯托尔机场的航班运行并没有因此次攻击事件而受到影响，但机场工作人员不得不为此采取应急措施——通过白板和记号笔来手动发布航班信息。

5.仅有 22 行的 Java 脚本让 38 万英国航空客户成为受害者

Cnbate 9 月 12 日消息，英国航空公司报告提到他们的其他服务，服务器或数据库都没有受到影响，这导致安全研究团队得出结论，支付服务是数据泄露的唯一罪魁祸首，这是 Magecart 熟知的专业领域。众所周知，这些骗子使用基于网络的卡片撇取器作为窃取信用卡支付数据的手段，这是经典的卡片撇取器的在线版本。

在深入研究英国航空公司网站内网络犯罪分子注入的代码之后，RiskIQ 研究人员发现仅有 22 行 JavaScript 代码是英国航空公司受该黑客攻击，导致 38 万名客户数据被盗的罪魁祸首。英国航空公司移动应用程序也受到改变的 Modernizr JavaScript 库的影响，因为它调用了网站使用的相同脚本资源，以允许客户进行付款。

研究人员表示，这次攻击再次向我们展示了黑客的高水平的规划和对细节的关注，这次攻击简单有效。研究人员还发现，所有被盗数据都被发送到位于罗马尼亚的服务器上的 baways.com 域，其 IP 地址为 89.47.162.248，由立陶宛 VPS（虚拟专用服务器）提供商 Time4VPS 提供。

此外，为了使 baways.com 域更可信，骗子使用了由 COMODO CA 发行的付费 SSL 证书，而不是购买免费的 LetsEncrypt 版本。 最近英国航空公司的数据泄露事件表明，Magecart 威胁行动者仍然是一个非常活跃的犯罪集团，据称他们已经在 2015 年开始活动并成功攻击了 Ticketmaster 和 Inbenta 等目标。

6.英国航空之后，Feedify 沦为 Magecart 黑客攻击的受害者

E 安全 9 月 14 日讯 据研究人员透露，继 Ticketmaster 和英国航空公司之后，推送通知服务 Feedify 沦为 Magecart 黑客攻击的最新受害者。Magecart 黑客组织将恶意代码添加到了 Feedify 客户嵌入其网站的文件当中。据传，Magecart 自 2015 年开始活跃，其最初两年的目标是 Magento 在线商店，2017 年底至 2018 年初开始改变策略，将目标瞄向主要服务，尤其托管 Web 基础设施。

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：刘立伟

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158