国家互联网应急中心

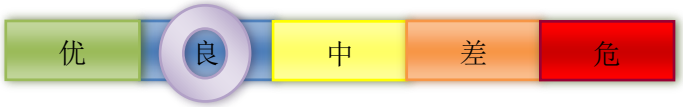
2018 年第 35 期

8 月 27 日-9 月 2 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

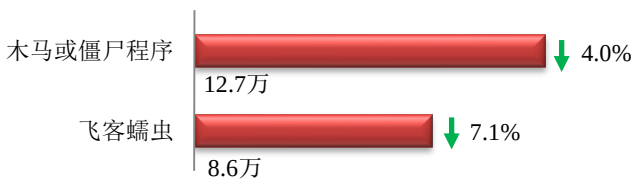


境内感染网络病毒的主机数量	•21.3万	5.3%
境内被篡改网站总数 其中政府网站数量	•760 •40	18.5% 17.6%
境内被植入后门网站总数 其中政府网站数量	•682 •24	15.4% 26.3%
针对境内网站的仿冒页面数量	•1914	21.0%
新增信息安全漏洞数量 其中高危漏洞数量	•356 •127	54.8% 69.3%

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*

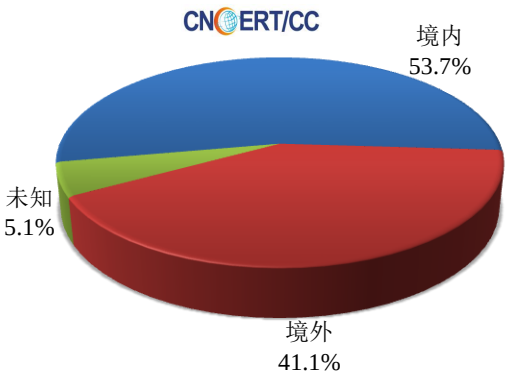
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 21.3 万个，其中包括境内被木马或被僵尸程序控制的主机约 12.7 万以及境内感染飞客（conficker）蠕虫的主机约 8.6 万。

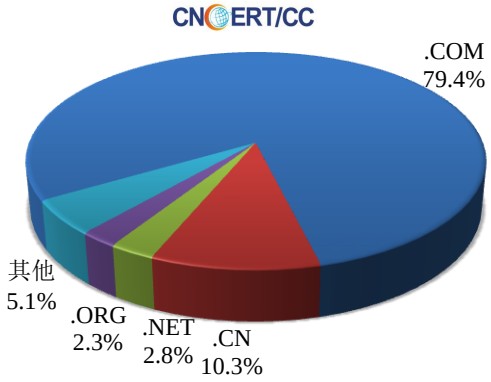


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 214 个，涉及 IP 地址 25182 个。在 214 个域名中，有 41.1%为境外注册，且顶级域为.com 的约占 79.4%；在 25182 个 IP 中，有约 20.6%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 60 个 IP。

本周放马站点域名注册所属境内外分布
(8/27-9/2)



本周放马站点域名所属顶级域的分布
(8/27-9/2)



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。

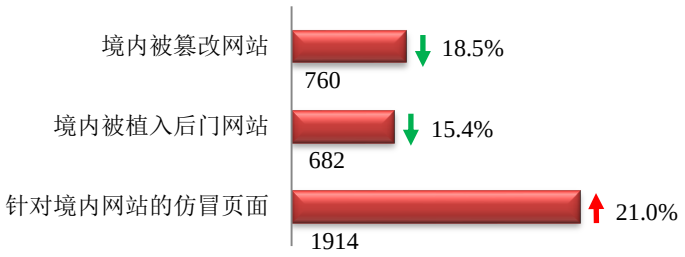
ANVA恶意地址黑名单发布地址

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。

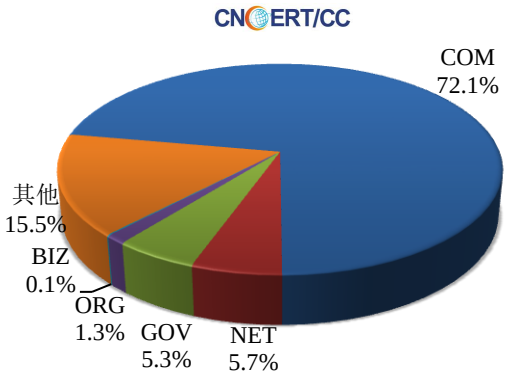
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 760 个；境内被植入后门的网站数量为 682 个；针对境内网站的仿冒页面数量为 1914。

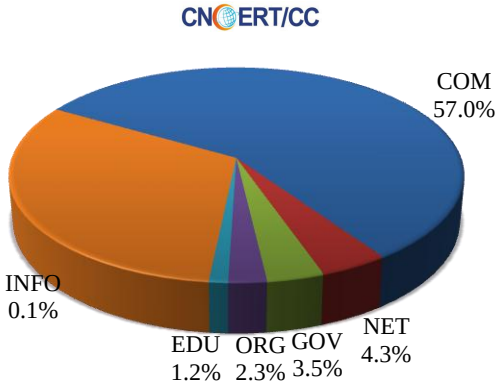


本周境内被篡改政府网站（GOV 类）数量为 40 个（约占境内 5.3%），较上周环比上升了 17.6%；境内被植入后门的政府网站（GOV 类）数量为 24 个（约占境内 3.5%），较上周环比上升了 26.3%；针对境内网站的仿冒页面涉及域名 633 个，IP 地址 311 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(8/27-9/2)

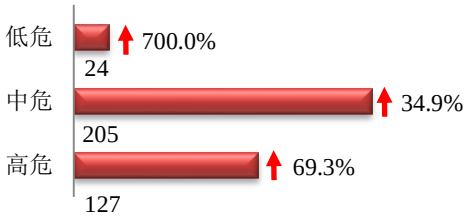


本周我国境内被植入后门网站按类型分布
(8/27-9/2)

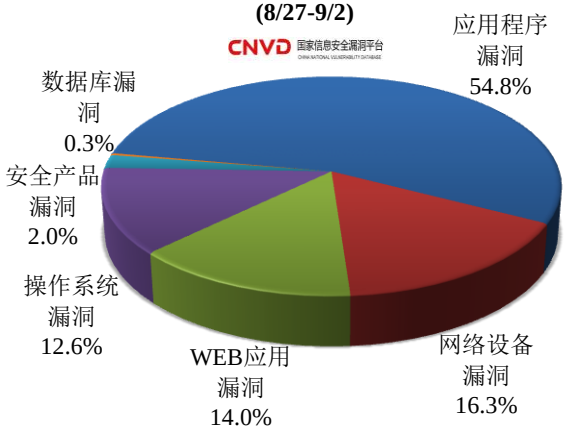


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 356 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
(8/27-9/2)



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

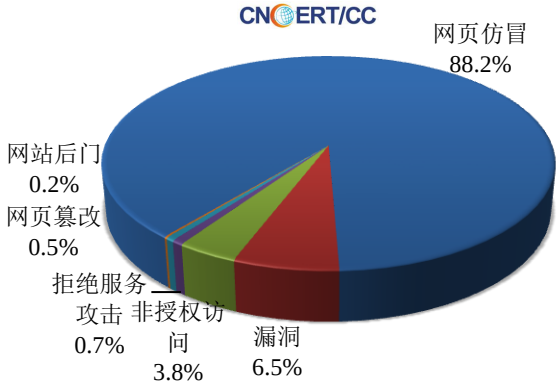
http://www.cnvd.org.cn/webinfo/list?type=4

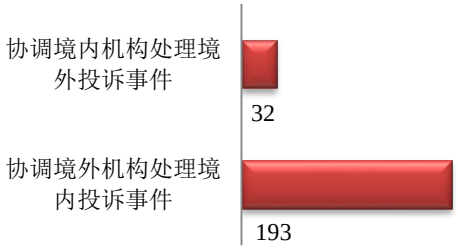
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 553 起，其中跨境网络安全事件 225 起。

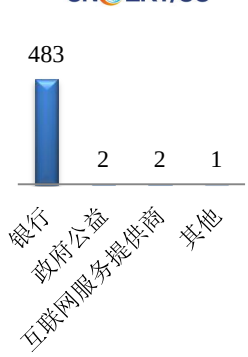
本周CNCERT处理的事件数量按类型分布 (8/27-9/2)



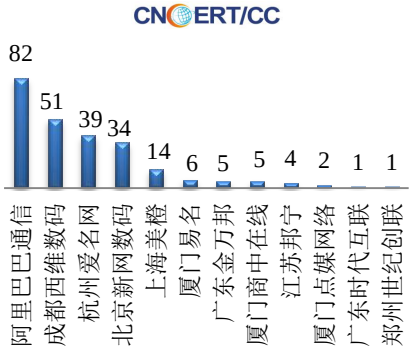


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 488 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 483 起和政府公益仿冒事件 2 起。

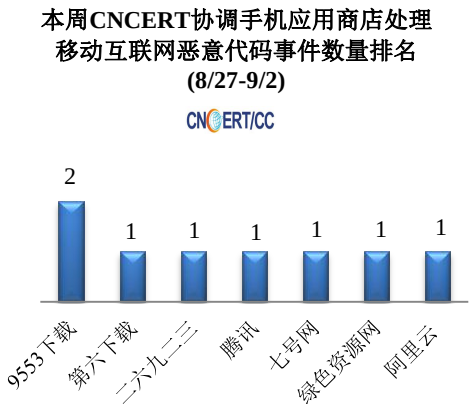
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(8/27-9/2)



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 (8/27-9/2)



本周，CNCERT 协调 7 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 8 个。



业界新闻速递

1、美国加州或将出台最严格的网络中立法案

E 安全 9 月 1 日消息 美国加利福尼亚州众议院 2018 年 8 月 30 日通过了一项法案，该法案不仅将恢复奥巴马颁布的网络中立保护规则，且有过之而无不及，可能会成为美国最严网络中立法案。这项法案将禁止互联网提供商阻止或限制任何合法的应用程序、网站或其他服务，并禁止有偿优先处理数据。该法案还需要回到参议院进行最后的投票，9 月 1 日即可见分晓。

2、德国成立新机构强化网络安全 结束对中美数字技术依赖

参考消息网 8 月 31 日消息 路透社 8 月 29 日报道称，德国 8 月 29 日宣布成立一个新机构，资助网络安全研究，结束对美国、中国和其他国家数字技术的依赖。内政部长霍斯特·泽霍费尔对记者说，德国需要新的工具来成为网络安全的顶级高手，并支持欧洲的安全和独立。报道称，泽霍费尔在与国防部长乌尔苏拉·冯德莱恩举行的记者会上说：“德国在国际层面，在网络安全方面发挥领导作用是我们的共同目标。我们必须承认我们落后了，在落后时就需要全新的方式。”该机构是内政部和国防部的联合项目。

3、以色列或全面改革网络监管，构建三级监管体系

E 安全 8 月 31 日消息 以色列国家安全研究所（INSS）的网络安全专家在一项新的研究中指出，虽然以色列在网络监管方面领先于许多国家，但以色列必须加快步伐改革这一进程。INSS 顶级网络安全专家 Gabi Siboni 表示，以色列虽然做了很多工作来保护国家基础设施和私营部门免受网络攻击，但这还远远不够。以色列目前甚至尚未出台全面的网络法，其 2018 年夏季提出的网络法案仍因各种隐私等问题而停滞不前。INSS 在研究中提出一个三级监管体系：第一级针对以色列国防军、以色列安全机构 Shin Bet、以色列情报机构 Mossad 和以色列警方，由其根据自身需求和风险自我监管；第二级涉及机构和私营企业，根据其重要性进行评级，根据评级

赋予适当的监管水平；第三级将减少监管，但在经济上予以激励，即通过税收减免或其他奖励或惩罚来满足最低限度的网络防御水平。

4、美国三大运营商被曝存在严重数据安全漏洞

腾讯网 8 月 27 日消息 据国外媒体报道称，本周对于电信公司来说并不顺利，因为有安全研究人员发现，AT&T、Sprint 和 T-Mobile 这三大美国电信运营商系统均存在安全漏洞，这些漏洞可能导致用户信息泄露。BuzzFeed 此前报道了两大可导致 AT&T 和 T-Mobile 客户信息容易受到黑客攻击的漏洞。黑客可以使用暴力破解工具来破解用户帐户、密码或者社保安全号码的最后四位数。另一大美国电信运营商 Sprint 内部员工帐户也存在漏洞。黑客可以利用员工设置的简易用户名和密码进入 Sprint 内部员工平台，且该公司并没有启用双重身份验证机制。黑客一旦进入内部系统，就可以访问包括 Sprint、BoostMobile 和 Virgin Mobile 在内的大量用户账户信息。研究人员还发现，任何获得访问权限的人都可以对用户账户进行更改，用户的密码可能会被暴力破解。

5、以色列士兵敏感数据遭遇黑客入侵

E 安全 8 月 28 日消息 以色列隐私保护局 8 月 26 日透露，数十万以色列士兵的个人数据几年来遭遇黑客入侵，并出售了第三方。以色列证券管理局（ISA）的调查显示，2011 年至 2014 年，征兵部门的工作人员访问了数千名以色列准士兵的档案。据以色列媒体报道，四名嫌疑人使用专门开发的程序从这些文件中搜索出个人数据，包括新兵及其亲属的联系人。嫌疑人称将此类信息出售了营销公司和其他第三方。

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：周昊

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158