国家互联网应急中心

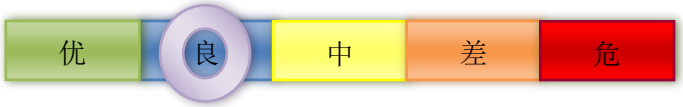
网络安全信息与动态周报

2018 年第 28 期

7 月 9 日-7 月 15 日

CNCERT/CC

本周网络安全基本态势

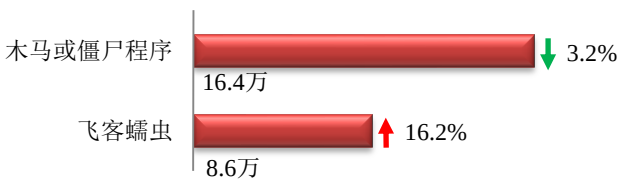


境内感染网络病毒的主机数量	•25.0万	2.7%
境内被篡改网站总数 其中政府网站数量	•996 •27	8.6% 15.6%
境内被植入后门网站总数 其中政府网站数量	•735 •12	19.1% 20.0%
针对境内网站的仿冒页面数量	•1158	14.0%
新增信息安全漏洞数量 其中高危漏洞数量	•257 •76	43.6% 38.2%

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

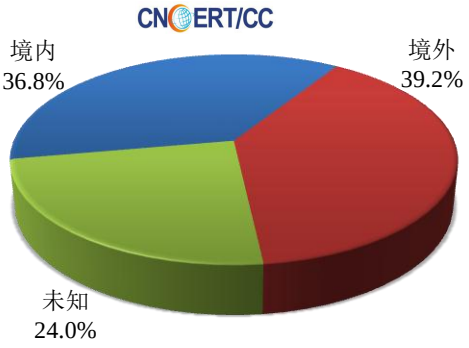
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 25.0 万个，其中包括境内被木马或被僵尸程序控制的主机约 16.4 万以及境内感染飞客（conficker）蠕虫的主机约 8.6 万。

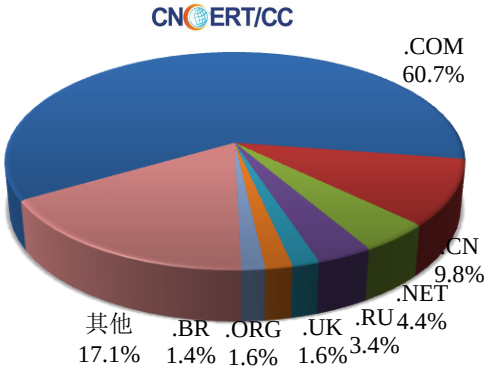


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 850 个，涉及 IP 地址 14568 个。在 850 个域名中，有 39.2%为境外注册，且顶级域为.com 的约占 60.7%；在 14568 个 IP 中，有约 47.4%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 163 个 IP。

本周放马站点域名注册所属境内外分布
(79-7/15)



本周放马站点域名所属顶级域的分布
(7/9-7/15)



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。

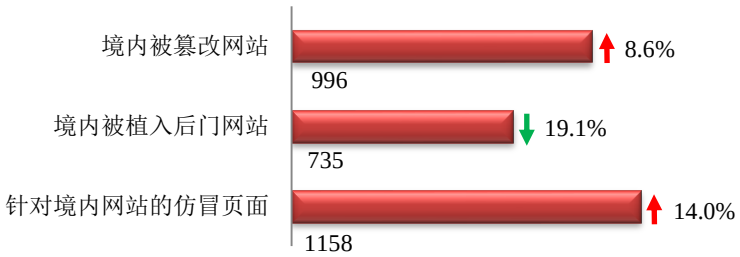
ANVA恶意地址黑名单发布地址

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。

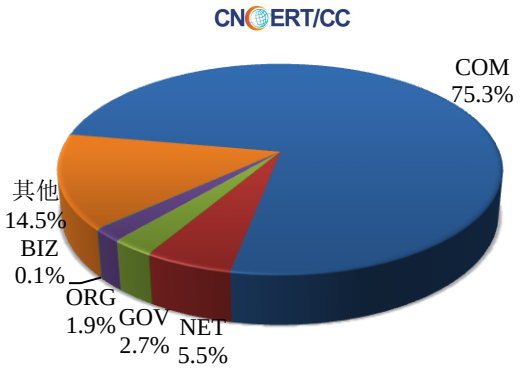
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 996 个；境内被植入后门的网站数量为 735 个；针对境内网站的仿冒页面数量为 1158。

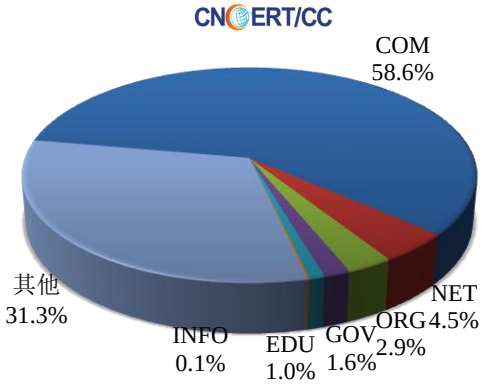


本周境内被篡改政府网站（GOV 类）数量为 27 个（约占境内 2.7%），较上周环比下降了 15.6%；境内被植入后门的政府网站（GOV 类）数量为 12 个（约占境内 1.6%），较上周环比下降了 20.0%；针对境内网站的仿冒页面涉及域名 420 个，IP 地址 196 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(7/9-7/15)

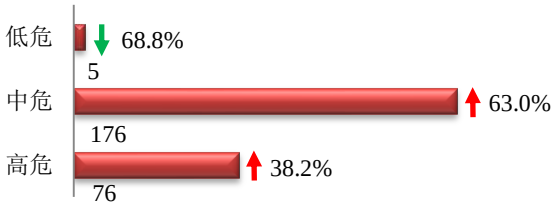


本周我国境内被植入后门网站按类型分布
(7/9-7/15)

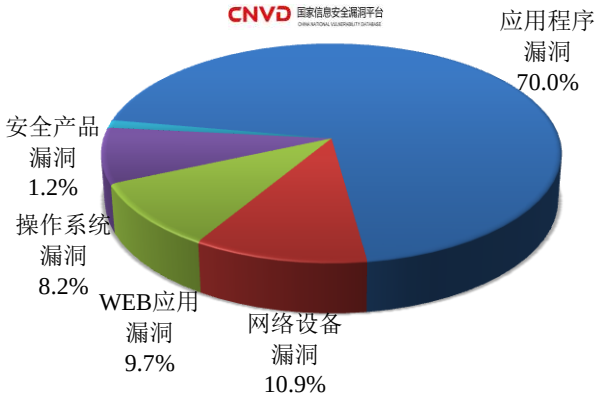


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 257 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
(7/9-7/15)



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

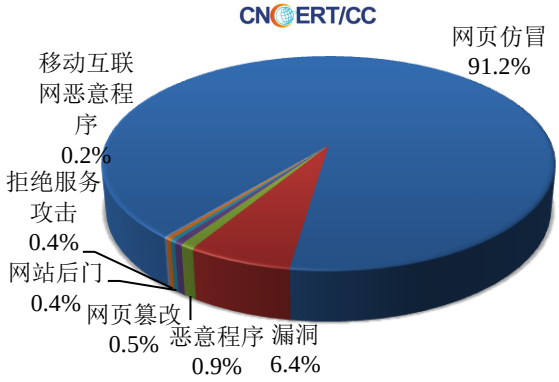
http://www.cnvd.org.cn/webinfo/list?type=4

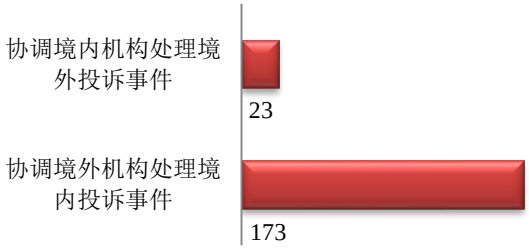
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 559 起，其中跨境网络安全事件 196 起。

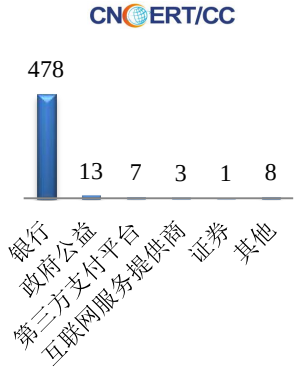
本周CNCERT处理的事件数量按类型分布 (7/9-7/15)



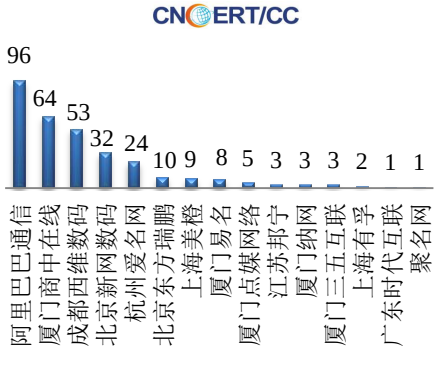


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 510 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 478 起和政府公益仿冒事件 13 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(7/9-7/15)

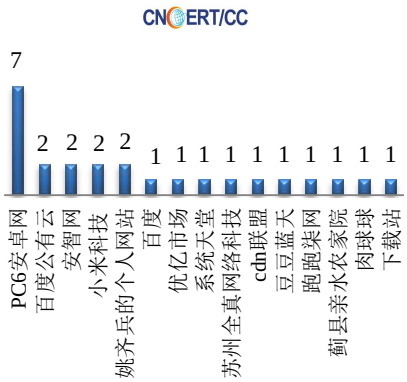


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (7/9-7/15)



本周，CNCERT 协调 15 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。

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
(7/9-7/15)



业界新闻速递

1、国内首次工业互联网安全防护演练在沪举行

中新网 7 月 11 日消息 国内首次针对工业互联网应用的安全防护演练活动 7 月 11 日在沪举行，活动由中国信息通信研究院与工业互联网产业联盟主办。中国工业和信息化部网络安全管理局副局长梁斌在发言时指出，随着互联网快速发展，大数据、人工智能等新型信息技术深刻改变生产方式，并由消费领域向生产领域快速蔓延。当前，中国正处于由网络大国向网络强国发展的关键时期，大力发展工业互联网的同时，安全保障至关重要；数据安全等成为工业互联网安全的焦点。作为新一代信息技术与制造业深度融合的关键载体，工业互联网是行业大势所趋，但安全问题不容忽视。当天的演练，旨在呈上一堂工业互联网安全普及教育课。现场，攻击实施团队利用工业互联网平台、工业控制系统和工业现场设备存在的安全漏洞，对相关企业的工业互联网平台以及生产管理系统模拟场景实施攻击，演示对工业互联网云、管、端多个层面的破坏和影响；现场技术防护团队实施了相应的技术防范措施，予以防护。

2、印度即将推行网络中立法

cnBeta.COM7 月 12 日消息 据外媒报道，印度电信部周三批准了网络中立规则。该规将让所有用户都能享受到访问网络内容的同等价格和速度。获悉，印度新法将禁止屏蔽、降级、减速或给予用户优惠待遇的网络使用情况存在。实际上印度一直都在推动这套网络中立法的推行。去年 11 月，印度电信监管部门建议，印度互联网访问应保持非歧视原则并且不能限制、屏蔽或给予优惠待遇。印度电信部长 Aruna Sundararajan 告诉媒体，任何违反网络中立规则的行为将都要受到严厉的惩罚。获悉，该套网络中立法将马上就要生效。不过该网络中立法也存在一些特例，像自动驾驶、远程医疗等新兴服务则拥有豁免权，因为它们可能需要更快的网络来展开各自的活动。

3、法国网络司令部首次加入巴黎巴士底日阅兵式

cnBeta.COM7 月 15 日消息 据外媒报道，日前，法国军事网络司令部首次参加了在巴黎香榭丽舍大街举行的巴士底日阅兵式。军方表示，这是对该部队自去年成立以来取得的进展的认可，另外它还强调网络防御将仍旧是该国处理的优先事项。法国国防部部长 Jean-Yves Le Drian 于 2016 年宣布了组建 COMCYBER 的消息。当时，这位部长指出，网络空间中国家行动者的出现是一种应对战争的新方式。该司令部在一个司令部下将全国所有士兵都集中到网络防御工作上，其中主要任务有三个：网络情报、保护和攻击。而法国创立这样一个司令部的时机并非巧合：此前美国曾指责俄罗斯干预了他们在 2016 年的总统大选。当地时间 7 月 13 日，这些指控获得了一些额外的可信支持，一个大陪审团公布了一系列针对 12 名俄罗斯人的指控，指控称这些俄罗斯人实施了网络攻击并破坏了美国的选举基础设施。

4、ISIS 欲发起“孤狼”行动，攻击西方基础设施

E 安全 7 月 10 日消息 据以色列《耶路撒冷邮报》获取的以色列国际反恐研究所（ICT）一份报告指出，伊斯兰网络恐怖分子正在加大力度对西方国家的基础设施发动网络攻击。研究人员对恐怖组织“伊斯兰国”（ISIS）所支持的黑客的账户进行监控，并在这份报告中讨论了恐怖分子网络行动的几种可能性，例如可能会在网上获取进攻能力以及出于该目的雇佣黑客或从支持恐怖主义的国家处获得援助。以色列国际反恐研究所（ICT）这份报告指出，网络恐怖主义进攻的另一个趋势是：“‘联合网络哈里发’（UCC）黑客组织的重组。虽然网络恐怖分子 2017 年初的攻击重点围绕社交网络账户进行，但年底就将重心转移至针对教育机构和关键基础设施的网络攻击。”

5、美空军遭黑客攻击 丢失极具杀伤力无人机敏感信息

海外网 7 月 11 日消息 美国网络安全公司“记录未来”（Recorded Future）最新研究显示，一名黑客侵入了美国空军上尉的电脑，窃取了有关美军极具杀伤力新型无人机的敏感信息。据美国有线电视新闻网（CNN）报道，被窃取的文件虽然没有分类，但其中包括一份 MQ-9A“收割者”无人机的飞行员名单以其他一些信息。“记录未来”公司研究员表示十分确定这名黑客来自南美，称这名黑客企图在“黑暗网站”上出售窃取的“收割者”无人机数据。该公司通过网上留言等方式与这名黑客取得了联系，并讨论了出售事宜。该黑客透露，他还窃取了美军爆炸装置的军事训练手册、坦克操作手册以及坦克排战术等相关文件，但他没有透露这些文件的来源。报道称，虽然被窃取的信息不是机密信息，但如果落入“不友好之人”的手里，对方就可以通过这些信息评估“收割者”无人机技术能力及其弱点。报道指出，美国执法部门目前已经介入调查。

6、德国托管服务提供商 DomainFactory 大量客户数据遭外泄

黑客视界 7 月 11 日消息 在上周，德国最大的托管服务提供商之一——DomainFactory，GoDaddy 旗下的子公司（在 2016 年被 Host Europe 收购）在其发布的公告中指出，一名匿名黑客在 DomainFactory 的技术支持论坛上发帖称，他已经成功侵入了 DomainFactory 的客户数据库。作为证据，黑客还分享了几名 DomainFactory 客户的内部数据。DomainFactory 最终在上周末确认了这一泄露事件，并公布了能够被黑客所访问的数据类型，这包括：客户名称，公司名称，客户帐户 ID，实际住址，电子邮件地址，电话号码，DomainFactory 手机密码，出生日期，银行名称及账号（如 IBAN 或 BIC），Schufa 得分（德国信用评分）。

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：张帅

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158