

网络安全信息与动态周报

本周网络安全基本态势



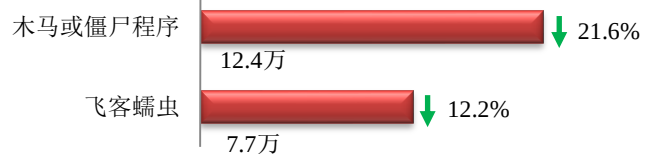
表示数量与上周相同

表示数量较上周环比增加

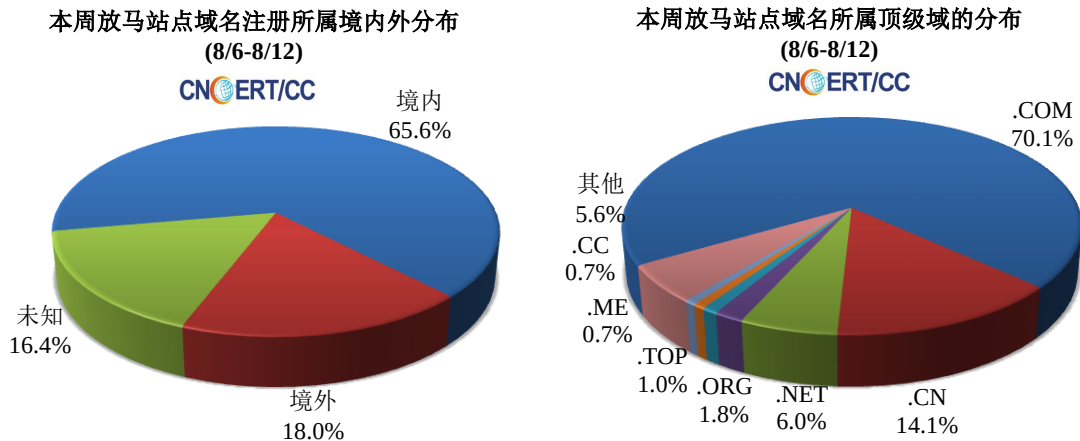
表示数量较上周环比减少

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 20.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 12.4 万以及境内感染飞客（conficker）蠕虫的主机约 7.7 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 822 个，涉及 IP 地址 48493 个。在 822 个域名中，有 18.0% 为境外注册，且顶级域为 .com 的约占 70.1%；在 48493 个 IP 中，有约 30.3% 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 120 个 IP。



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。

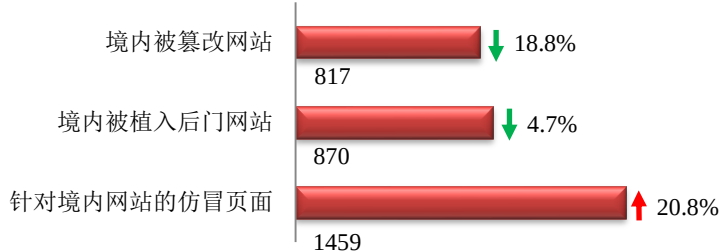
ANVA 恶意地址黑名单发布地址

<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。

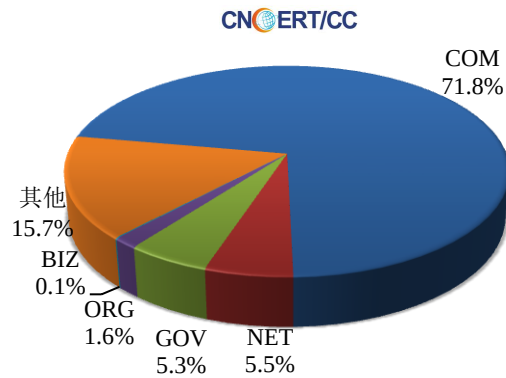
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 817 个；境内被植入后门的网站数量为 870 个；针对境内网站的仿冒页面数量为 1459。

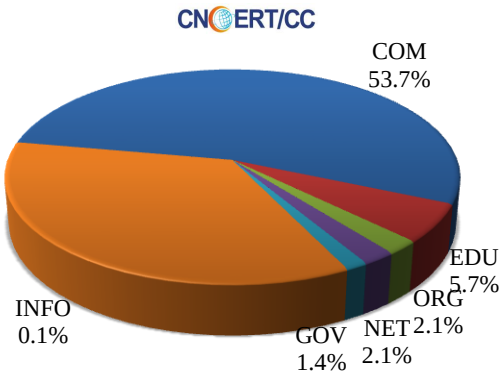


本周境内被篡改政府网站（GOV 类）数量为 43 个（约占境内 5.3%），较上周环比上升了 19.4%；境内被植入后门的政府网站（GOV 类）数量为 12 个（约占境内 1.4%），较上周环比上升了 33.3%；针对境内网站的仿冒页面涉及域名 637 个，IP 地址 232 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(8/6-8/12)

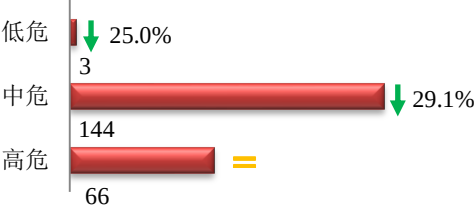


本周我国境内被植入后门网站按类型分布
(8/6-8/12)

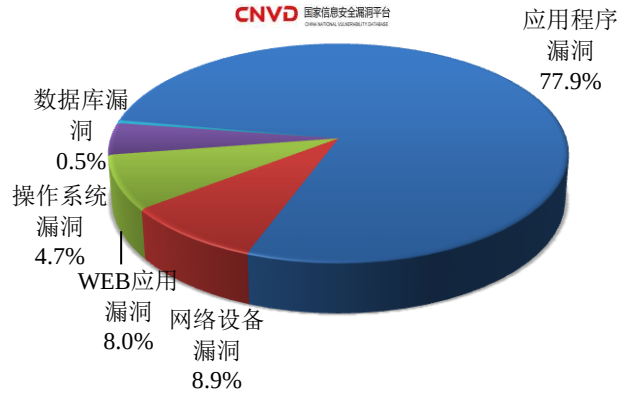


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 213 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
(8/6-8/12)



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

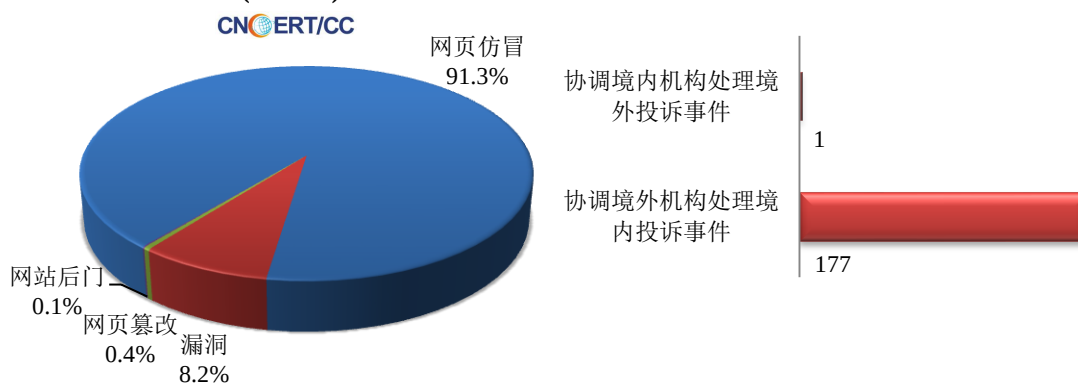
<http://www.cnvd.org.cn/webinfo/list?type=4>

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

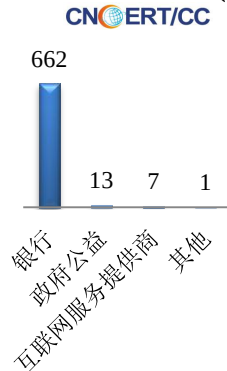
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 748 起，其中跨境网络安全事件 178 起。

本周CNCERT处理的事件数量按类型分布
(8/6-8/12)

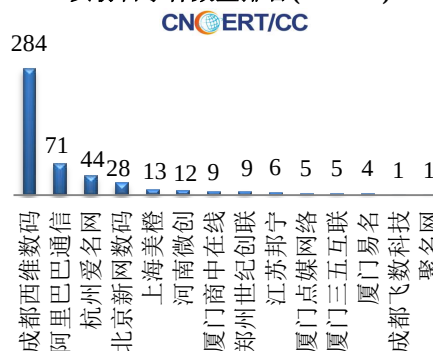


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 683 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 662 起和政府公益仿冒事件 13 起。

本周CNCERT处理网页仿冒事件数量
按仿冒对象涉及行业统计(8/6-8/12)

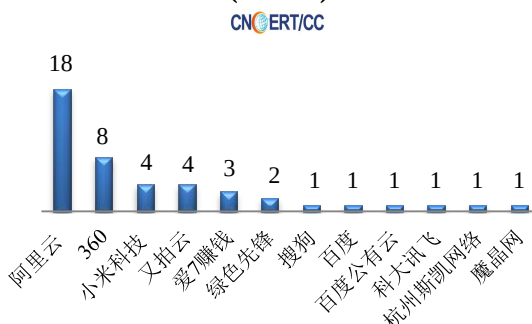


本周CNCERT协调境内域名注册机构处理网
页仿冒事件数量排名 (8/6-8/12)



本周，CNCERT 协调 12 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 45 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
(8/6-8/12)



业界新闻速递

1、美国防部机构联合英国公司研发 AI 网络安全技术

中新网 8 月 9 日消息 据侨报网报道，美国国防部高级计划研究局（DARPA）联手英国 BAE 系统公司正在研发一种新的人工智能（AI）网络安全技术，以应对当今日益复杂且频繁的高级别网络攻击。美媒称，这个被称为“精准网络狩猎”（Cyber Hunting at Scale，简称 CHASE）的研发项目旨在采用计算机自动化，先进算法和一种新的速度处理标准，来实时跟踪大量数据，帮助安全人员锁定那些采用高级别黑客技术且隐藏在大量数据流中的网络攻击。DARPA 将这一技术解释为“自适应数据收集”技术，既通过 AI 技术自动筛选大量信息，而非人工来“跟踪”并进行实时调查。DARPA CHASE 项目经理罗伯茨（Jennifer Roberts）在一份书面声明中说：“CHASE 项目的宗旨就是寻求开发自动化工具来检测和明确新的攻击向量，同时收集正确的上下文数据，并在企业内部和企业间传播安全保护措施。”

2、欧盟要求成员国将网络安全立法转为国家法律

中国信息产业网 8 月 6 日消息 据欧盟官网消息，近日欧盟委员会向 17 个成员国发出正式通函，要求其将欧盟首个网络安全立法，即“欧盟网络和信息系統安全指令”（NIS Directive）完全转为国家法律。据悉，这 17 个成员国分别为：奥地利、保加利亚、比利时、克罗地亚、丹麦、法国、希腊、匈牙利、爱尔兰、拉脱维亚、立陶宛、卢森堡、荷兰、波兰、葡萄牙、罗马尼亚和西班牙。欧洲议会全体会议 2016 年 7 月 6 日通过“欧盟网络和信息系統安全指令”（NIS Directive），旨在欧盟范围内实现一体的高级别网络和信息安全系统，提升成员国网络安全能力，加强欧盟网络和信息安全合作。2016 年 8 月，安全指令正式生效，并要求所有成员国在 2018 年 5 月 9 日前将其转为国家法律。截至目前，有 11 个成员国通知欧委会已完成法律转化，并在进行转化后的评估程序，以确认是否完全转化。在接到欧委会的正式通函后，尚未完成法律转化的 17 个成员国需在 2 个月之内就通函回复。欧委会若未接到回复，将向其发出理由意见书。

3、FBI 全球部署，挫败网络犯罪“独角兽” Fin7

E 安全 8 月 8 日消息 近日，目前为止组织最为严密的复杂网络犯罪组织 Fin7（也被称为 Anunak、银行大盗 Carbanak）黑客集团三名核心成员被美国联邦调查局（FBI）逮捕。如果人们谈论网络犯罪集团，还将他们看作是初创公司，那么 Fin7 黑客集团会被认为是十亿级的独角兽，该黑客集团被认为是目前为止组织最为严密的复杂网络犯罪组织。该集团自 2014 年开始就开始进行国家级的黑客活动，其利用钓鱼和社工技术窃取银行账户和信用卡卡号，然后从全球各地的银行和企业窃取了数亿资金。2018 年 7 月 29 日，FBI 宣布逮捕了该黑客集团的三名高级成员（44 岁的 Dmytro Fedorov，33 岁的 Fedir Hladyr 和 30 岁的 Andrii Kopakov），对该团伙造成了毁灭性打击。

4、香港卫生署遭勒索软件攻击，官方称暂无资料外泄

黑客视界 8 月 6 日消息 据《南华早报（SCMP）》报道，香港卫生署已成为黑客攻击的最新受害者，此前有三台计算机遭到勒索软件攻击，导致数据无法被访问，目前警方已经就此事展开了刑事调查。香港卫生署证实，自上个月 15 日起，共有三个部门（感染控制处、药物办公室和临床遗传服务处）的三台计算机先后因感染勒索软件而导致文件被加密。黑客留下了自己电子邮件地址，以便获取加密密钥，但并没有标注赎金的具体金额。卫生署的一位发言人称，这几台计算机都不包含任何敏感的个人信息，并且初步调查的结果显示也不存在任何资料外泄。另外，由于卫生署会定期对计算机中的文件进行备份，因此受影响的工作人员可以从备份中取回所需的文件。

5、台积电核心工厂感染电脑病毒一度停工 损失上亿

环球网 8 月 7 日消息 据《日本经济新闻》8 月 7 日报道，全球最大半导体代工企业台湾积体电路制造(简称台积电、TSMC)发布消息称，其台湾主力工厂感染计算机病毒，8 月 6 日一度停产。受到的影响按销售额计算最多达到 190 亿日元。台积电 CEO 魏哲家 6 日在台北市内举行记者会称，本次事件将对部分供货造成影响。魏哲家针对感染的原因解释称，是人为失误，让没有充分杀毒的设备与系统连接导致。本次的病毒是 2017 年在世界范围内大爆发的“WannaCry”病毒的变种。

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：雷君

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158

