国家互联网应急中心

2018 年第 2 期

1 月 8 日-1 月 14 日

网络安全信息与动态周报

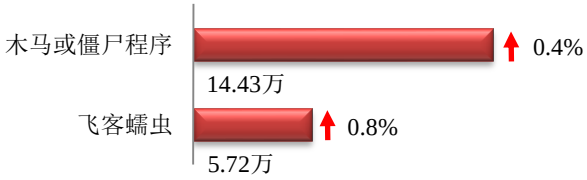
本周网络安全基本态势

境内感染网络病毒的主机数量	•20.15万	↑ 0.5%
境内被篡改网站总数 其中政府网站数量	•2117 •44	↓ 4.2% =
境内被植入后门网站总数 其中政府网站数量	•773 •32	↓ 6.5% ↓ 15.8%
针对境内网站的仿冒页面数量	•419	↑ 2.9%
新增信息安全漏洞数量 其中高危漏洞数量	•257 •109	↑ 17.4% ↑ 73.0%

=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

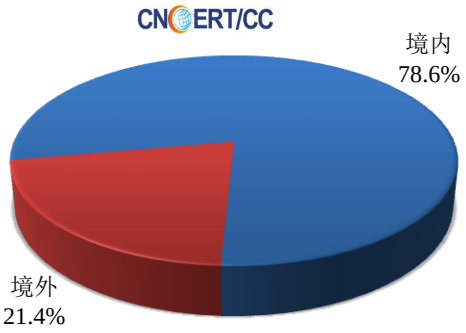
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 20.15 万个，其中包括境内被木马或被僵尸程序控制的主机约 14.43 万以及境内感染飞客（conficker）蠕虫的主机约 5.72 万。

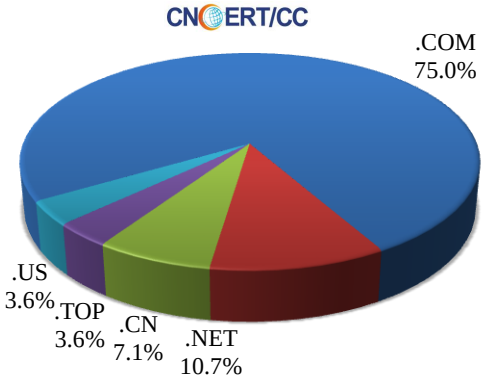


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 28 个，涉及 IP 地址 122 个。在 28 个域名中，有 21.4%为境外注册，且顶级域为.com 的约占 75.0%；在 122 个 IP 中，有约 26.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 1 个 IP。

本周放马站点域名注册所属境内外分布
(1/8-1/14)



本周放马站点域名所属顶级域的分布
(1/8-1/14)



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。

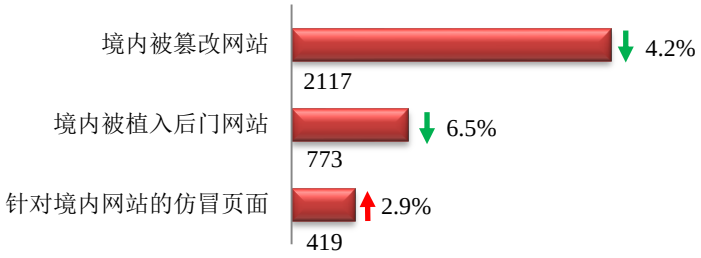
ANVA恶意地址黑名单发布地址

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。

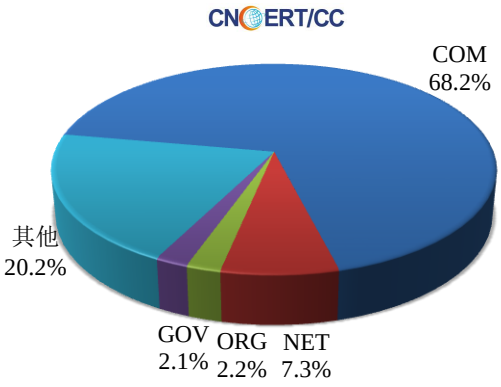
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 2117 个；境内被植入后门的网站数量为 773 个；针对境内网站的仿冒页面数量为 419。

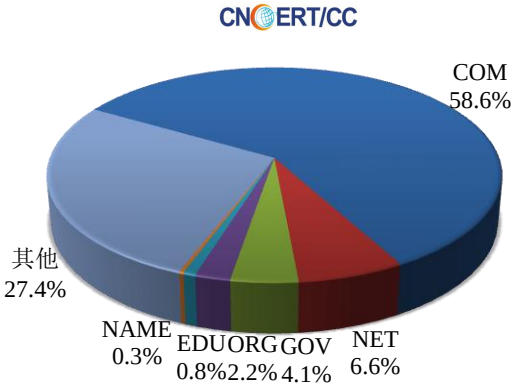


本周境内被篡改政府网站（GOV 类）数量为 44 个（约占境内 2.1%），与上周持平；境内被植入后门的政府网站（GOV 类）数量为 32 个（约占境内 4.1%），较上周环比下降了 15.8%；针对境内网站的仿冒页面涉及域名 323 个，IP 地址 158 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(1/8-1/14)

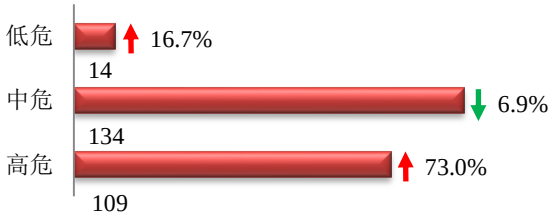


本周我国境内被植入后门网站按类型分布
(1/8-1/14)

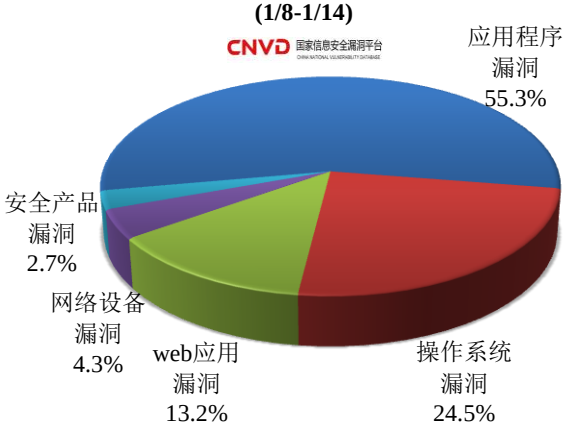


本周重要漏洞情况

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高。



本周CNVD收录漏洞按影响对象类型分布
(1/8-1/14)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是操作系统漏洞和 web 应用漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

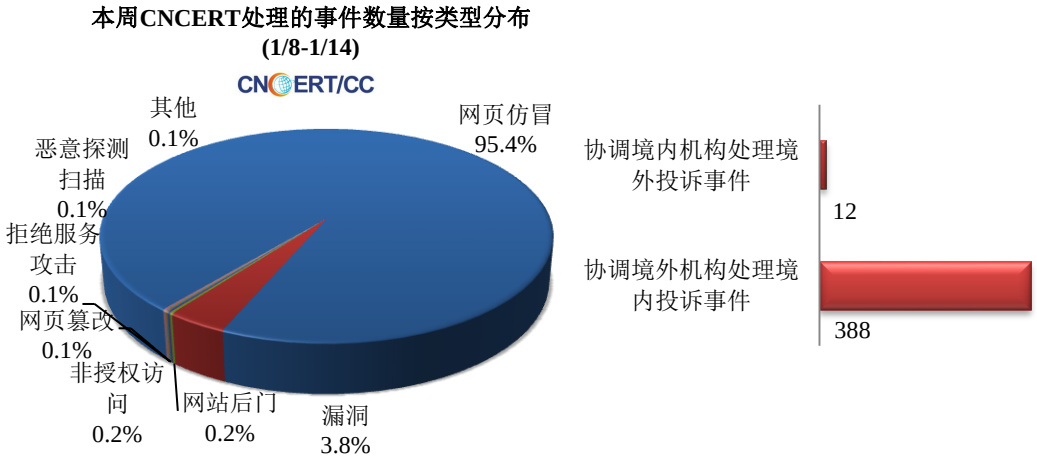
CNVD漏洞周报发布地址

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。

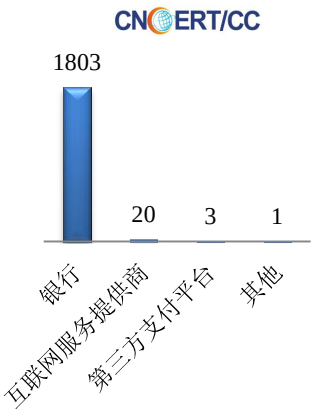
本周事件处理情况

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 1918 起，其中跨境网络安全事件 400 起。

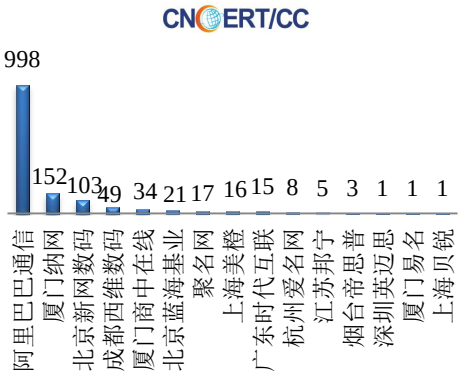


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1827 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 1803 起和互联网服务提供商仿冒事件 20 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(1/8-1/14)

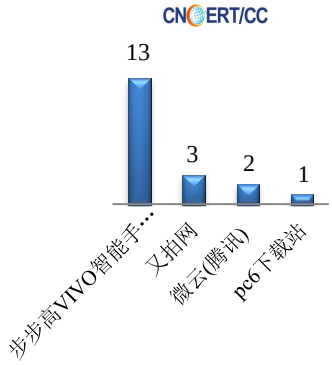


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (1/8-1/14)



本周，CNCERT 协调 4 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 19 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 (1/8-1/14)



业界新闻速递

1、欧盟关键信息基础设施之 NIS 指令

E 安全 1 月 8 日消息 2017 年，关于欧盟“数据保护条例 GDPR”热议之声在网络安全领域达到峰值，使得关于 GDPR 的讨论甚至盖过了另一项同样重要的欧盟相关法令的风头——欧盟“网络与信息安全（NIS）指令”。2018 年将成为 NIS 指令正式生效的元年，网络安全业界将借助此项新的网络安全立法把握新的机遇。NIS 指令属于欧盟网络安全立法中的第一部分，该指令要求到 2018 年 5 月 9 日，全部欧盟成员国都必须将其纳入本国法律当中。对于网络安全行业来说，NIS 应该比 GDPR 获得更多的关注。NIS 指令更侧重于保护社会进展的一大核心因素：关键信息基础设施。NIS 指令的目标在于立足三个方面改善关键信息基础设施水平：各欧盟成员国国家网络安全能力（例如其必须拥有国家级 CSIRT 并执行网络演习等等）；欧盟各成员国之间需要跨境合作（例如欧盟 CSIRT 运营网络、NIS 战略合作组织等）；对各关键性部门（包括能源、运输、水资源、卫生以及金融等）以及关键性数字化服务供应商（包括互联网交换点以及域名系统等）的运营实施国家级网络安全监管。

2、日本自卫队“网军”花 8000 万引入人工智能 参考美以技术

参考消息网 1 月 8 日消息 日媒称，记者 1 月 6 日获悉，为强化应对网络攻击的能力，日本防卫省已经决定从 2021 年度起，在控制自卫队网络防御部队信息通信网络的系统中引入人工智能。据日本《产经新闻》1 月 7 日报道，从下一年度开始，日本防卫省计划用两年时间开展调查研究，2019 年度起着手开发相关软件，2021 年度正式投入使用。此外还计划将人工智能广泛用于防御所有政府部门的网络。报道称，自卫队引进人工智能用于维护虚拟空间安全，就是期待其在检测未知病毒、预测将要遭受到的攻击等方面发挥作用。2018 年度预算案中编入了 8000 万日元的调研经费，参考对象为在网络空间防御和人工智能方面领先的美国、以色列等国的技术。

3、日本开发新型加密技术 号称量子计算机也难破解

新浪网 1 月 8 日消息 日本总务省下属的信息通信研究机构开发出了新型加密技术，连新一代超高速计算机——量子计算机也难以破解。该技术的原理是将需要保护的信息转换为特殊的数学问题，可代替通信网等现有加密技术来使用。这项技术已入选新一代加密技术的国际标准候选方案，将成为物联网（IoT）的基础技术，为保护网上交易等的机密性发挥重要作用。此次开发的新型加密技术可按照一定规律将密码及信用卡号等需要保护的数字转换成其他数字。只要拥有解码“密钥”就能马上解开，但如果第三方通过计算机计算来强行破解密码，只要解不开数学上的难题，就无法破解。

4、澳大利亚政府发布小型企业网络安全指南

E 安全 1 月 11 日消息 近日，澳大利亚政府小型企业与家族企业监察专员组（ASBFEO）发布了小型企业网络安全指南——《网络安全最佳实践指南》。这份指南囊括了“自我保护”的三个步骤，旨在帮助澳大利亚国内的各小型企业运营人员预防或更好地应对网络攻击活动，帮助受众了解当前风险以及如何防范网络攻击活动。澳大利亚小型企业与家族企业监察专员凯特·卡内尔认为，有相当一部分小型企业缺乏足够的时间与资源，而网络犯罪活动正变得愈发复杂，因此小型企业更容易受到此类活动的影响。在线威胁已经与物理威胁一样真实存在，网络安全问题需要得到认真对待。卡内尔还表示，小型企业不应畏惧“走向网络”，因为网络当中蕴藏着巨大的发展机遇与利益。众多小型企业已经成功开设虚拟店铺与实体店面结合发展，进而建立起可持续的运营模式。

5、外媒：芯片漏洞被公开之后 英特尔将在内部新建一个网络安全部门

新浪网 1 月 9 日消息 1 月 9 日消息，据国外媒体报道，在芯片中发现的漏洞被公开之后，英特尔除了发布补丁修复发现的漏洞，还在公司结构上进行调整，将在公司内部新建一个网络安全部门。外媒的报道显示，英特尔 CEO 布莱恩•科再奇周一向员工发送了一份备忘录，备忘录的主要内容就是在公司内部新建一个负责网络安全的部门。据悉，英特尔在内部新建的网络安全部门名为“英特尔产品保证与安全”，这一新部门将由英特尔人力资源主管莱斯利•库伯斯通（Leslie Culberstone）负责领导。

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。截止 2016 年，CNCERT 与 69 个国家和地区的 185 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：李佳

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158