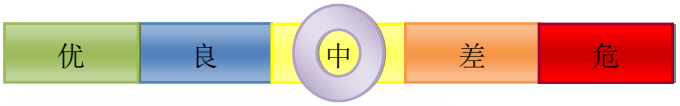
国家互联网应急中心

2019 年第 41 期
10 月 7 日-10 月 13 日

网络安全信息与动态周报

本周网络安全基本态势

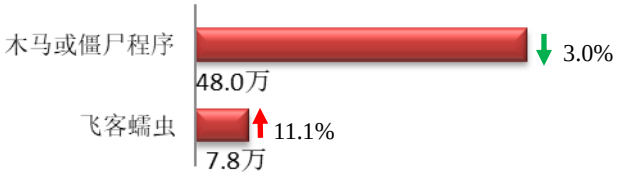


境内感染网络病毒的主机数量	•55.9 万	↓1.2%
境内被植入后门网站总数 其中政府网站数量	•2682 •11	↓6.3% ↓54.5%
针对境内网站的仿冒页面数量	•351	
新增信息安全漏洞数量 其中高危漏洞数量	•488 •116	

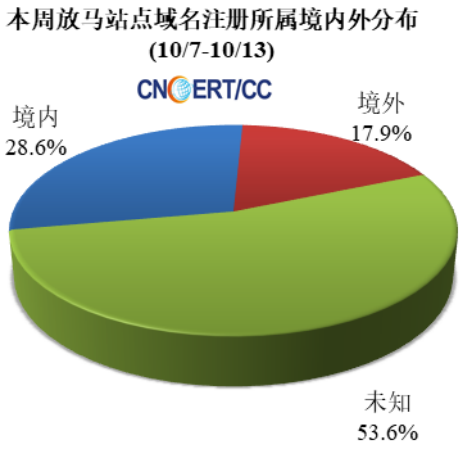
═表示数量与上周相同　↑表示数量较上周环比增加　↓表示数量较上周环比减少

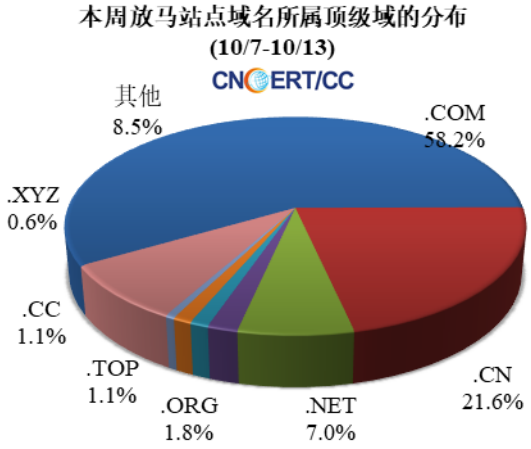
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 55.9 万个，其中包括境内被木马或被僵尸程序控制的主机约 48.0 万以及境内感染飞客（conficker）蠕虫的主机约 7.8 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 704 个，涉及 IP 地 1657 个。在 704 个域名中，有 17.9%为境外注册，且顶级域为.com 的约占 58.2%；在 1657 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 170 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。

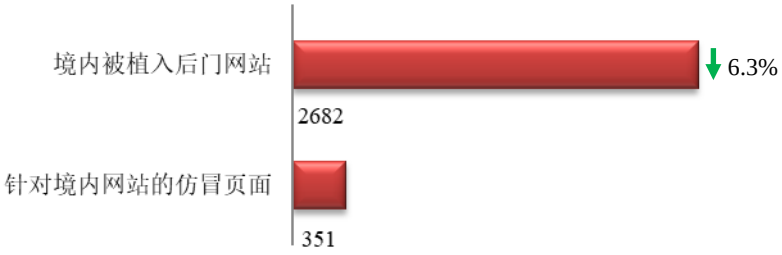
ANVA恶意地址黑名单发布地址

http://www.anva.org.cn/virusAddress/listBlack

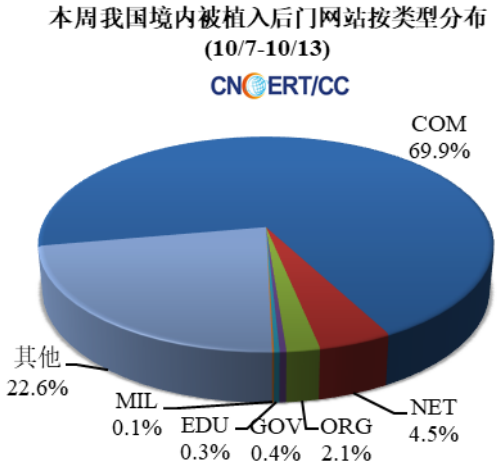
中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由中国互联网协会网络与信息安全工作委员会发起、CNCERT 具体组织运作的行业联盟。

本周网站安全情况

本周 CNCERT 监测发现境内被植入后门的网站数量为 2682 个；针对境内网站的仿冒页面数量 351 个。

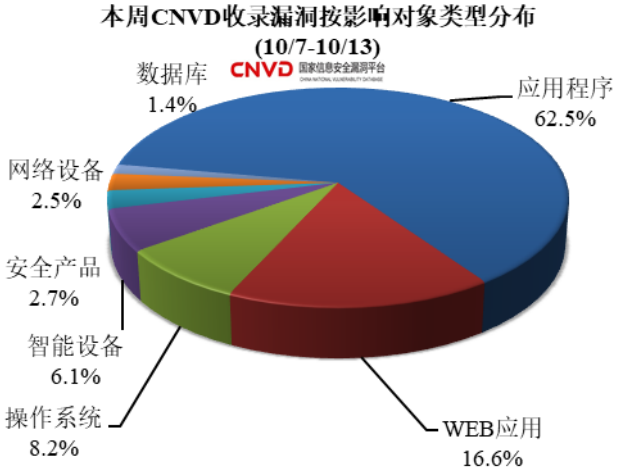


本周境内境内被植入后门的政府网站（GOV 类）数量为 11 个（约占境内 0.4%），较上周环比上涨 37.5%；针对境内网站的仿冒页面涉及域名 205 个，IP 地址 128 个，平均每个 IP 地址承载了约 3 个仿冒页面。



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 488 个，信息安全漏洞威胁整体评价级别为中。



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 应用漏洞和操作系统。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

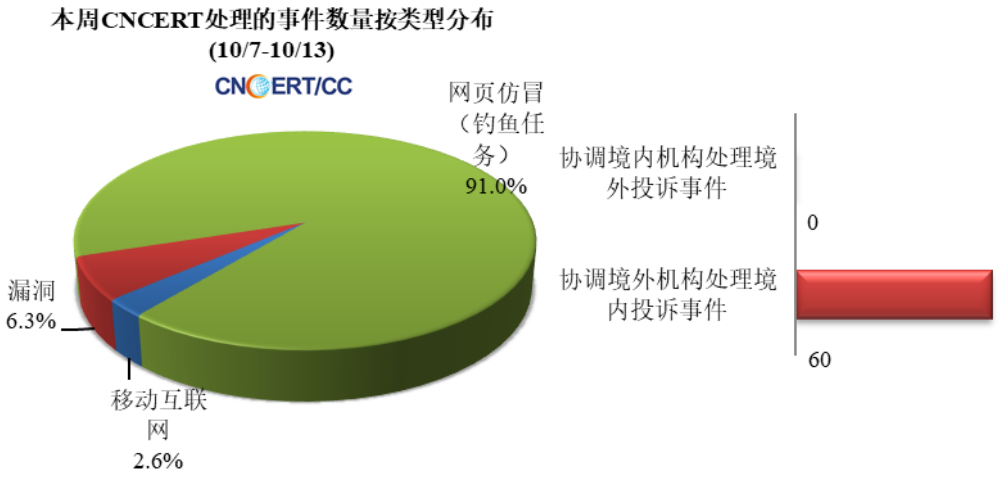
CNVD漏洞周报发布地址

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

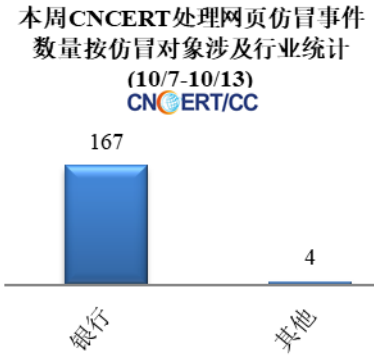
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

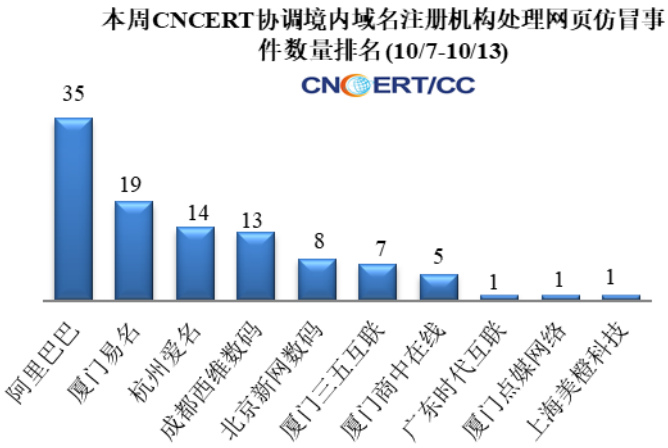
本周事件处理情况

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 189 起，其中跨境网络安全事件 60 起。

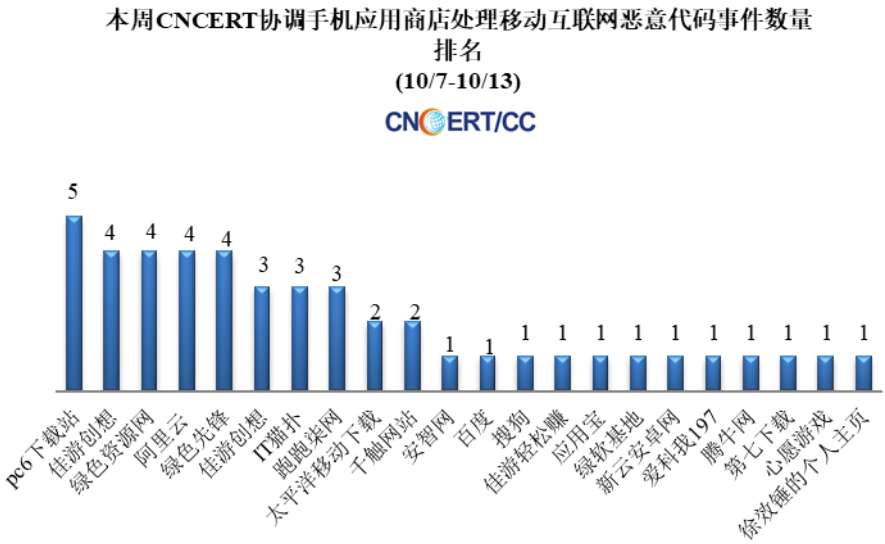


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 171 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 167 起和其他仿冒事件 4 起。





本周，CNCERT 协调 22 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 46 个。



业界新闻速递

2、国际刑警组织报告：勒索软件仍是网络安全最大威胁

10 月 9 日新华网消息，欧洲刑警组织 9 日于当天开幕的第七届欧洲刑警组织-国际刑警组织网络犯罪议题大会上与国际刑警组织共同发布题为《2019 互联网有组织犯罪威胁评估》这一报告，指出勒索软件仍是网络安全最大威胁，全球各界需加强合作打击网络犯罪。报告指出，数据已成为网络犯罪分子的主要攻击目标。此外，防范针对智能城市的勒索软件攻击成为一个重点。报告说，2019 年最明显的勒索软件攻击是针对地方政府，这对全球城市都是一种警示。

1、惠普电脑的预装应用出现漏洞，或将允许黑客完全接管系统

10 月 11 日 Techrepublic 官网消息，SafeBreach Labs 的安全研究人员披露，惠普电脑的一个预装应用中存在一个本地特权提升漏洞（CVE-2019-6333），该漏洞允许攻击者通过预装在大多数惠普电脑上的 HP Touchpoint Analytics 软件进行提权，以此绕过安全机制进行攻击。

研究人员发现，当 HPTouchpoint Analytics 被激活时，该应用将尝试加载已经丢失的 DLL 文件。黑客便可将恶意 DLL 文件的名称改为丢失文件的名称，再自动执行恶意文件指令。一旦入侵成功，黑客便能够轻易将自身权限提升至 SYSTEM 级，从而绕过各种防御措施，乃至接管系统。据 SafeBreach 估计，因为所有旧版本（4.1.4.2827 以下）的 HPTouchpoint Analytics 都存在此漏洞，所以将有数千万台惠普电脑受到波及。目前，惠

普已经发布了 HP Touchpoint Analytics Client 4.1.4.2827 版本，用以修复漏洞。

3、三星：20 多处安全漏洞影响所有 Galaxy 旗舰机型

10 月 9 日《福布斯》报道，三星日前证实，发现多处安全漏洞影响 Galaxy S8、S9、S10、S10e、S10Plus、S105G、Note9、Note10 和 Note10Plus 等型号手机。这其中，包括一个非常严重的漏洞(critical vulnerability)，以及三个被评为“高危”(high)的漏洞。整体而言，它们涉及到约 21 个安全问题，其中 17 个与三星“One”用户界面有关，4 个与 Android 有关。关于 Android 的漏洞，谷歌上周已经公布，攻击者正利用谷歌 Android 移动操作系统中的“零日漏洞”进行攻击，该漏洞可以让他们完全控制至少 18 种不同型号的手机，包括四个型号的 Pixel 手机，以及三星 Galaxy S7、S8 和 S9。三星的 Galaxy 特定安全警告，三星最新的安全维护版本(SMR)现已开始向所有 Galaxy 设备用户推出。

4、俄罗斯电信公司 Beeline 曝出数据泄露事故

10 月 7 日《莫斯科时报》消息，黑客从俄罗斯电信供应商 Beeline 窃取了 870 万用户的数据，并将其在网上出售、共享。报道指出，Beeline 公司在俄罗斯、亚洲地区以及澳大利亚提供电信服务，其在俄罗斯地区的用户数量可达 5000 万。据报道，此次泄露事故发生于 2017 年，但该公司一直未将其公布于众。该公司表示，此事故将影响在 2016 年 11 月之前注册家庭宽带连接的俄罗斯用户，被泄露的信息包括用户全名、住址、手机和固定电话号码，以及其他用户个人信息。此前还有报道称，黑客试图出售俄罗斯联邦储蓄银行 6000 万用户的敏感信息。

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：李金凝

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315