国家互联网应急中心

2019 年第 6 期

2 月 4 日-2 月 10 日

网络安全信息与动态周报

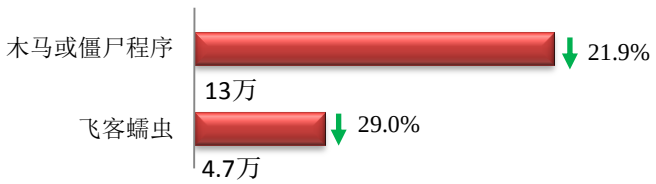
本周网络安全基本态势

境内感染网络病毒的主机数量	•17.8万	↓ 23.9%
境内被篡改网站总数 其中政府网站数量	•608 •37	↓ 1.6% ↑ 8.8%
境内被植入后门网站总数 其中政府网站数量	•354 •0	↓ 16.5% ↓ 100.0%
针对境内网站的仿冒页面数量	•350	↑ 9.4%

═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

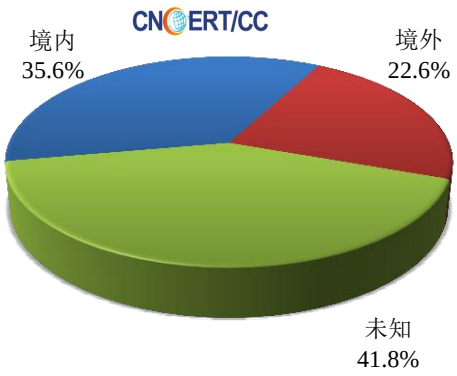
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 17.8 万个，其中包括境内被木马或被僵尸程序控制的主机约 13.0 万以及境内感染飞客（conficker）蠕虫的主机约 4.7 万。

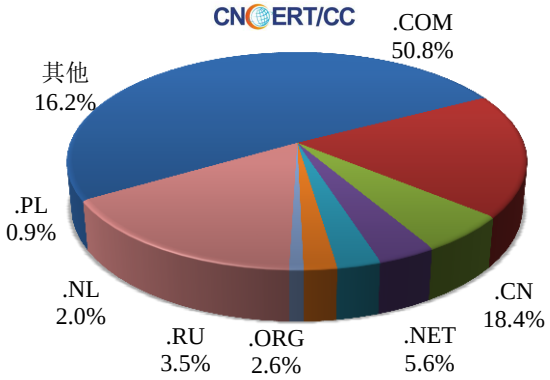


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 2453 个，涉及 IP 地址 4660 个。在 2453 个域名中，有 22.6%为境外注册，且顶级域为.com 的约占 50.8%；在 4660 个 IP 中，有约 50.0%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 352 个 IP。

本周放马站点域名注册所属境内外分布
(2/4-2/10)



本周放马站点域名所属顶级域的分布
(2/4-2/10)



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。

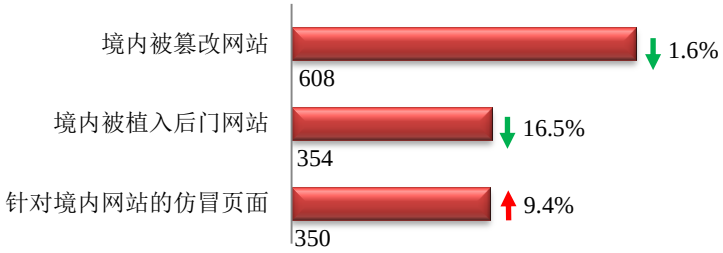
ANVA恶意地址黑名单发布地址

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。

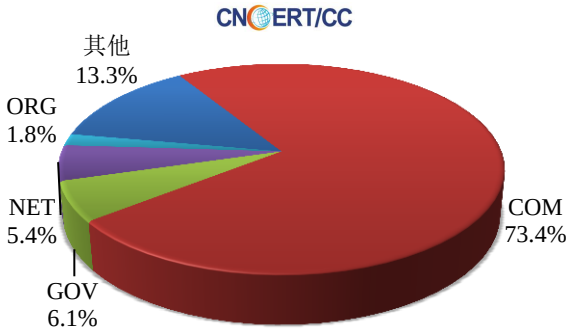
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 608 个；境内被植入后门的网站数量为 354 个；针对境内网站的仿冒页面数量 199 个。

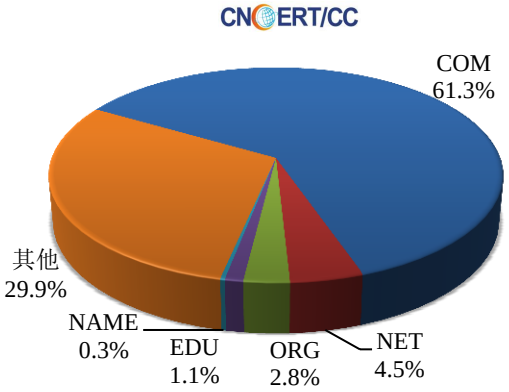


本周境内被篡改政府网站（GOV 类）数量为 37（约占境内 6.1%），较上周环比上升了 8.8%；境内被植入后门的政府网站（GOV 类）数量为 0 个（约占境内 0.0%），较上周环比下降了 66.7%；针对境内网站的仿冒页面涉及域名 76 个，IP 地址 36 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(2/4-2/10)



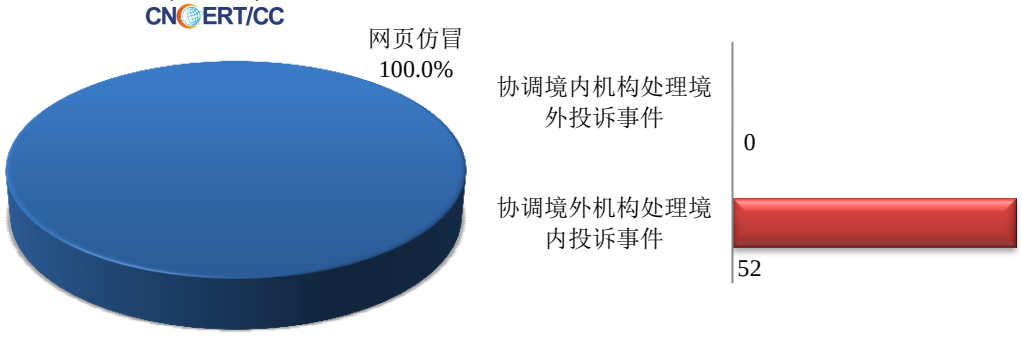
本周我国境内被植入后门网站按类型分布
(2/4-2/10)



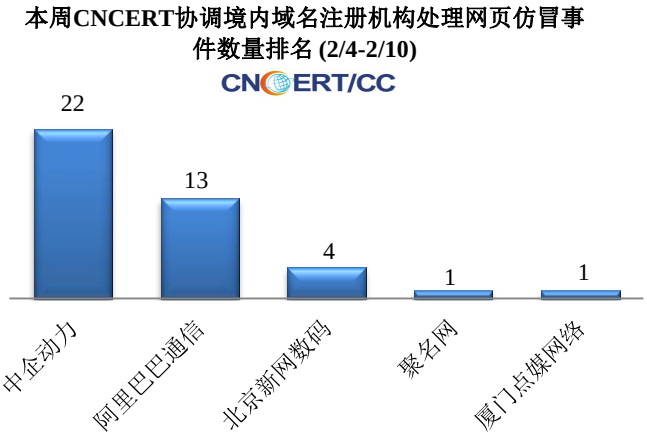
本周事件处理情况

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 122 起，其中跨境网络安全事件 52 起。

本周CNCERT处理的事件数量按类型分布
(2/4-2/10)



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 122 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 122 起。



业界新闻速递

1、肯尼亚国家身份证强制关联 DNA

cnBeta.COM2 月 10 日消息 Mozilla 对肯尼亚的新国家身份证发出了警告。肯尼亚议会上个月通过了对国家身份法的修订，国家综合身份管理系统（National Integrated Identity Management System，缩写 NIIMS）现在要求所有肯尼亚人，移民和难民交出 DNA，住宅地址 GPS 坐标、视网膜扫描、虹膜，语音波形和耳垂几何图。NIIMS 将整合其它政府数据库信息，生成名为 Huduma Namba 的唯一识别码。修正案是在没有公开辩论的情况下通过的，Mozilla 对中心化身份识别系统的安全问题、监控问题和歧视问题提出了担忧，认为推行数字身份识别系统至少需要配合强有力的隐私数据保护法规。

2、Enox 儿童智能手表存在严重隐私安全问题 欧盟下令全面召回

cnBeta.COM2 月 6 日消息 欧洲委员会宣布一项大规模召回通知，要求旗下成员国全面召回由德国公司 Enox 制造的 Safe Kid One 儿童智能手表，这也是欧盟首次因为隐私问题而全面召回的产品。据媒体报道，RAPEX 机构上周发出安全警告，指 Safe KID One 产品有严重隐私漏洞，以没有加密的方式与服务器通信，被黑客利用或者截获都可直接获得佩戴者（儿童）的定位数据和电话，修改手表序号等。欧洲委员会下令立即全面召回这款产品。

3、戴尔拟出售网络安全公司 SecureWorks

凤凰科技 2 月 8 日讯 戴尔公司正在计划出售美国网络安全服务提供商 SecureWorks Corp，其市值接近 20

亿美元。戴尔持有 SecureWorks 85%的股权，此次交易将使戴尔得以削减其 500 亿美元的债务。该公司去年计划通过“反向收购”其子公司 VMware Inc.完成 IPO。据报道，戴尔将与投资银行摩根士丹利合作完成交易，目前交易仍处于早期阶段。

4、xDedic 被 FBI 等机构联合查抄

cnBeta.COM2 月 4 日消息 联邦调查局与来自几个欧洲国家的监管当局一起查抄了 xDedic 的域名和服务器，xDedic 是一个臭名昭着的在线市场，网络犯罪分子会出售并购买被黑客服务器的访问权限。三名嫌犯也在乌克兰被捕。该网站作为一个在线市场运作，其中几个犯罪集团出售或购买被黑客入侵的服务器，通常采用被接管的 RDP（远程桌面协议）账户的形式。该网站列出了近 7 万台黑客服务器，每台服务器的价格仅为 8 美元。根据 2017 年的 Flashpoint 报告，xDedic 服务器数量后来上升至 85000 个，而价格最低单价为 6 美元。调查人员表示，xDedic 列出了来自全球各地的服务器，其中包括地方，州和联邦政府基础设施，医院，紧急服务，主要大城市交通管理部门，会计和律师事务所，养老基金和大学网络上的受感染计算机。

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：胡俊

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158