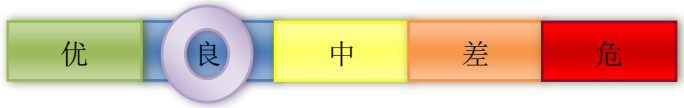
国家互联网应急中心

2019 年第 2 期

1 月 7 日-1 月 13 日

网络安全信息与动态周报

本周网络安全基本态势

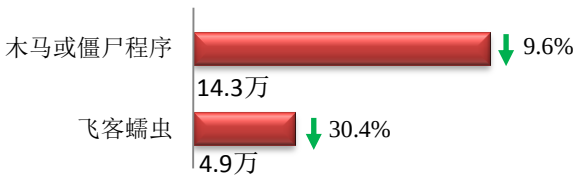


境内感染网络病毒的主机数量	• 19.2万	↓ 9.6%
境内被篡改网站总数 其中政府网站数量	• 690 • 41	↑ 3.1% ↓ 21.2%
境内被植入后门网站总数 其中政府网站数量	• 805 • 17	↑ 45.6% ↑ 70.0%
针对境内网站的仿冒页面数量	• 3634	↑ 23.6%
新增信息安全漏洞数量 其中高危漏洞数量	• 225 • 68	↑ 63.0% ↑ 54.5%

= 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

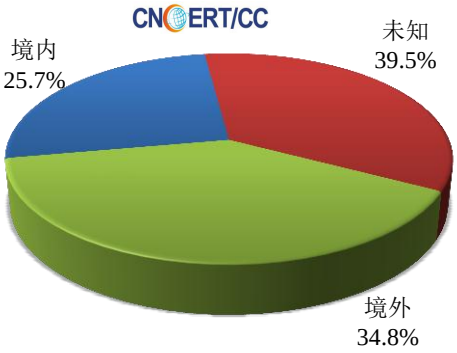
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 19.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 14.3 万以及境内感染飞客（conficker）蠕虫的主机约 4.9 万。

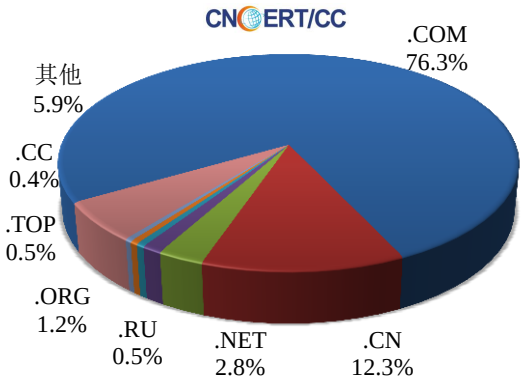


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 2825 个，涉及 IP 地址 2600 个。在 2825 个域名中，有 34.8%为境外注册，且顶级域为.com 的约占 76.3%；在 2600 个 IP 中，有约 53.0%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 301 个 IP。

本周放马站点域名注册所属境内外分布
(1/7-1/13)



本周放马站点域名所属顶级域的分布
(1/7-1/13)



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。

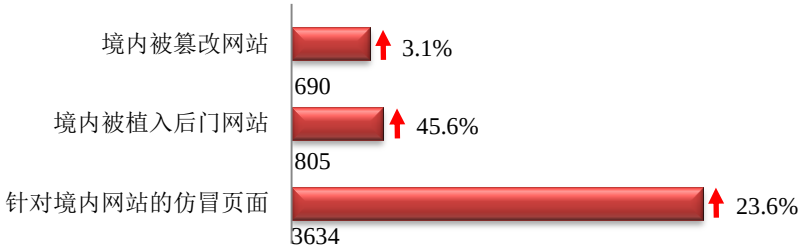
ANVA恶意地址黑名单发布地址

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。

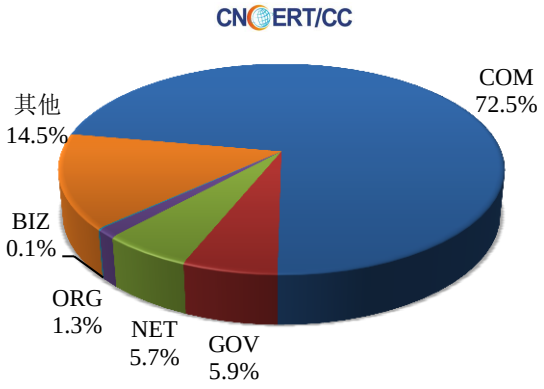
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 690 个；境内被植入后门的网站数量为 805 个；针对境内网站的仿冒页面数量 3634 个。

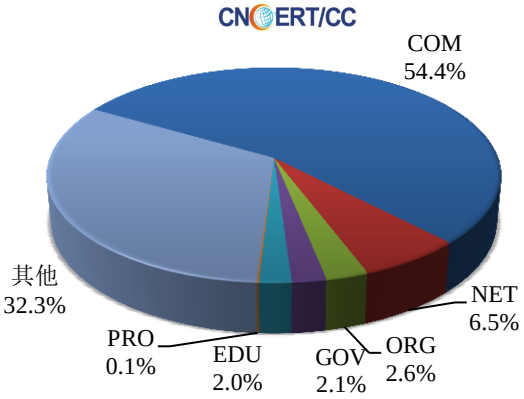


本周境内被篡改政府网站（GOV 类）数量为 41 个（约占境内 5.9%），较上周环比下降了 21.2%；境内被植入后门的政府网站（GOV 类）数量为 17 个（约占境内 2.1%），较上周环上升了 70.0%；针对境内网站的仿冒页面涉及域名 1166 个，IP 地址 296 个，平均每个 IP 地址承载了约 44 个仿冒页面。

本周我国境内被篡改网站按类型分布
(1/7-1/13)

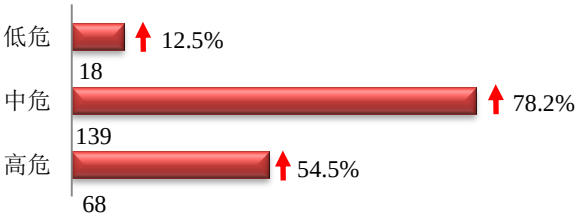


本周我国境内被植入后门网站按类型分布
(1/7-1/13)

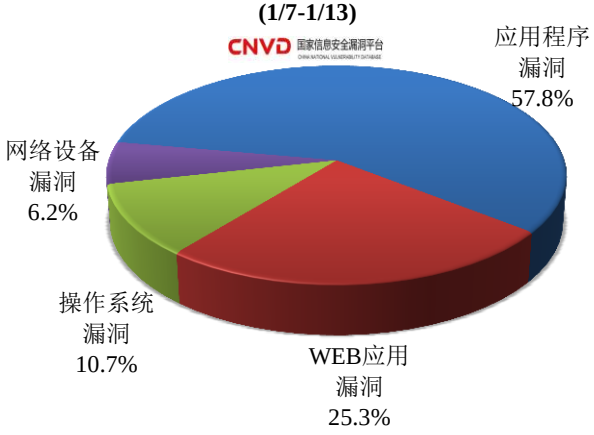


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 225 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
(1/7-1/13)



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 应用程序漏洞和操作系统漏洞。

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

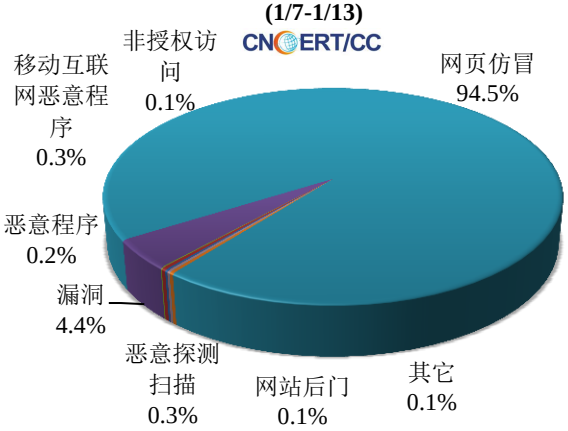
http://www.cnvd.org.cn/webinfo/list?type=4

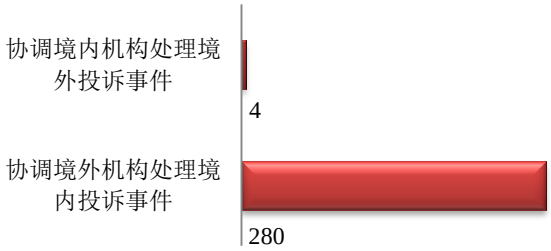
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 1021 起，其中跨境网络安全事件 284 起。

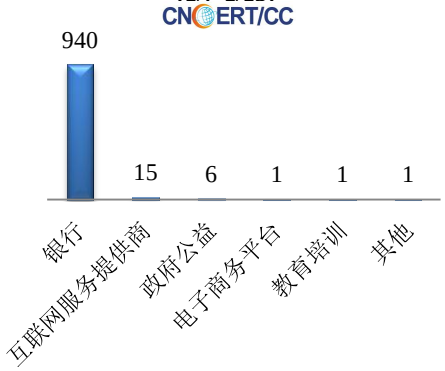
本周CNCERT处理的事件数量按类型分布 (1/7-1/13)



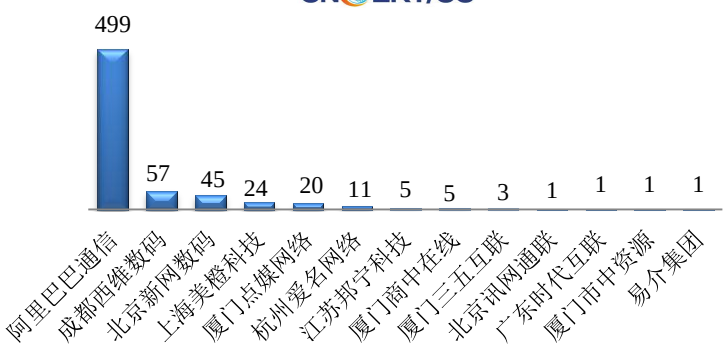


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 964 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 940 起和互联网服务提供商仿冒事件 15 起。

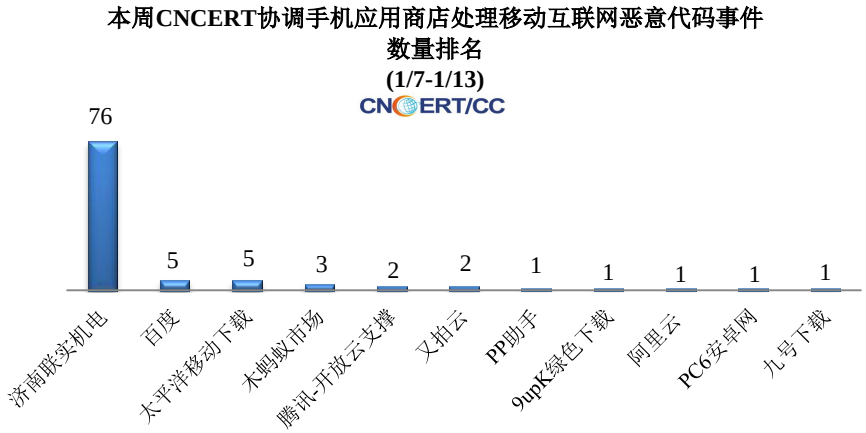
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (1/7-1/13)



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 (1/7-1/13)



本周，CNCERT 协调 11 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 98 个。



业界新闻速递

1、芬兰和印度将加强在网络安全和空间领域的合作

E 安全 1 月 12 日消息 据芬兰外交部报道，芬兰常务国务秘书 Matti Anttonen 于 2019 年 1 月 8 日至 10 日对印度进行了访问。1 月 10 日，芬兰国务秘书 Anttonen 与印度外交国务部长 Vijay Kumar Singh 举行了会谈，双方签署了两份谅解备忘录，一份关于网络安全领域的合作，一份关于太空的和平利用。芬兰交通运输局国家网络安全中心（TrafiCom）和印度计算机应急响应小组（CERT-In）将共同处理网络安全的文件。该谅解备忘录表达了双方在网络安全事务中开展更密切合作的愿景。在网络社会中，一个部门所面临的网络威胁通常也会影响到其他部门。双方合作的目的是加强双方在各种网络威胁方面的信息交流，提高防范和解决网络安全事件的能力。芬兰在网络安全事务方面的专业技能闻名世界。

2、美国政府关门导致许多 TLS 证书到期让网站无法访问

cnBeta.COM1 月 12 日消息 美国政府关闭导致国家公园和政府部门无人值守，今天是数十万联邦工人不会收到薪水的第一个发薪日。关闭的另一个副作用是许多政府网站因其 TLS 证书已过期而处于脱机状态，并且没有人可以续订它们。网站受影响的机构包括美国航空航天局，美国司法部和上诉法院。据 Netcraft 称，总共有大约 80 个或更多的 TLS 证书已经过期，这使得许多站点无法被公众访问。

3、美国加州保险局网站存漏洞，或已暴露数万人的个人信息

安全内参 1 月 13 日消息，印度网络安全公司 Banbreach 就一个美国加州保险局（California Department of Insurance，CDI）网站漏洞与网络安全博客 DataBreaches.net 取得了联系。据 Banbreach 称，在早前已经通知了 CDI，一个连接到 interactive.web.insurance[.]gov 的 Oracle 报表服务器在 24 小时内生成了 24450 多份报表，而该

服务器能够被公开访问。通过这个网站漏洞暴露的其他报告被描述为：保险索赔调查报告，包括姓名、车辆登记号码和住址等详细信息；保险索赔调查报告，包括姓名、车辆登记号码和住址等详细信息；关于月度欺诈的统计报告；被起诉人的详细个人信息，以及指控的细节（如罪名、罚款等）。

4、加拿大保守党参议员推特账户被黑，个人信息遭曝光

黑客视界 1 月 9 日消息 据加拿大 CTV 新闻台报道，保守派参议员琳达·弗拉姆（Linda Frum）的推特账户在上周日夜间遭到了黑客攻击，一群黑客通过她的推特账户分享了包括她的驾照扫描件在内的个人信息，并通过她的推特账户发布了种族歧视语言。为了解决此类问题，加拿大政府提出了 C-76 综合法案，其中就包括采取措施来使选举更加现代化。这项立法提出了一项新的妨害计算机信息系统罪，旨在遏制来自其他国家的黑客干扰加拿大的选举进程。

5、NASA 内部应用程序泄露 NASA 员工和项目数据

E 安全 1 月 13 日消息 据外媒报道，NASA 内部应用程序——JIRA 出现了一个严重的配置错误，导致内部数据泄露，任何人都可以访问这些数据。JIRA 是一个由 Atlassian 公司支持的项目管理系统，可进行 bug 跟踪和敏捷项目管理。这个出现错误的配置用于管理 NASA 内部员工和项目信息。泄露的数据包含高度敏感的信息，包括内部用户详细信息、项目详细信息、员工姓名、员工邮箱 id。错误配置导致互联网上的任何人都能访问 NASA 的内部数据，这也为网络罪犯提供了访问的机会。根据研究人员的说法，此次信息泄露是由于 JIRA 全局权限设置中的授权配置错误造成的。控制面板中配置为“所有用户”和“所有人”可见。与此同时，公共用户可以更改 JIRA 中的设置，以获得完整的员工用户名和密码列表。研究人员表示，黑客可以通过这个漏洞知道在 JIRA 中包含哪些类型的信息，项目团队正在处理哪些项目，以及不同项目的性质。

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：姚力

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158