国家互联网应急中心

网络安全信息与动态周报

2019 年第 21 期

5 月 20 日-5 月 26 日

CNCERT/CC

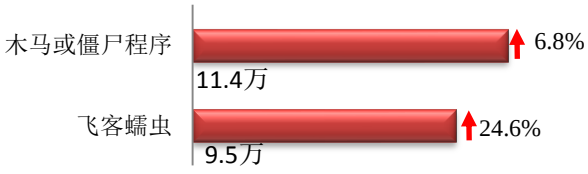
本周网络安全基本态势

境内感染网络病毒的主机数量	•20.9万	↑ 14.2%
境内被篡改网站总数[1] 其中政府网站数量	•9337 •18	↑ 533.4% ↑ 1700.0%
境内被植入后门网站总数 其中政府网站数量	•1176 •12	↑ 9.2% ↑ 50.0%
针对境内网站的仿冒页面数量	•2392	↑ 116.3%
新增信息安全漏洞数量 其中高危漏洞数量	•271 •74	↓ 25.3% ↓ 33.3%

=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

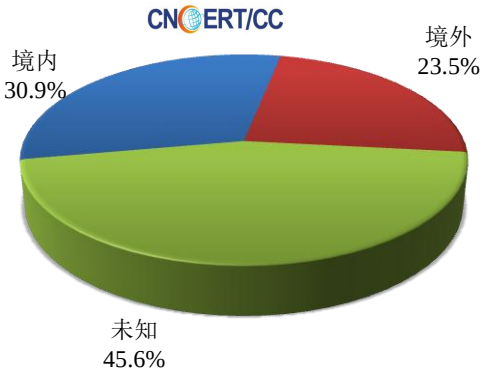
本周境内感染网络病毒的主机数量约为 20.9 万个，其中包括境内被木马或被僵尸程序控制的主机约 11.4 万以及境内感染飞客（conficker）蠕虫的主机约 9.5 万。



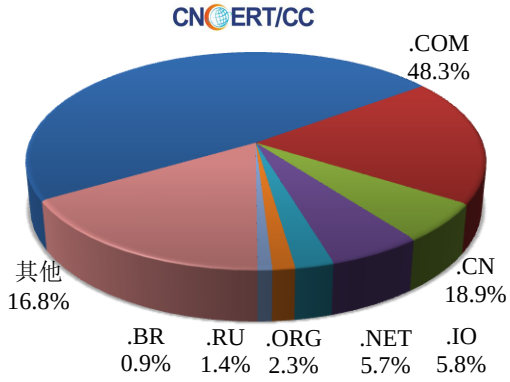
[1]本期境内被篡改网站数量受监测数据范围扩大影响，波动较大

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 4096 个，涉及 IP 地址 6287 个。在 4096 个域名中，有 23.5%为境外注册，且顶级域为.com 的约占 48.3%；在 6287 个 IP 中，有约 57.4%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 681 个 IP。

本周放马站点域名注册所属境内外分布
(5/20-5/26)



本周放马站点域名所属顶级域的分布
(5/20-5/26)



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。

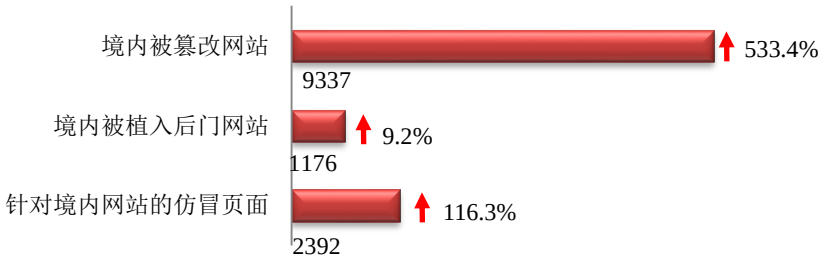
ANVA恶意地址黑名单发布地址

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。

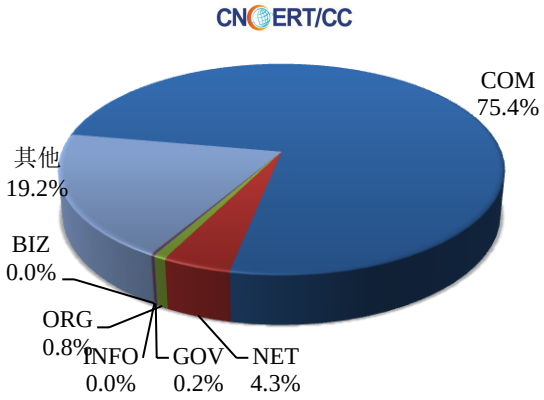
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 9337 个；境内被植入后门的网站数量为 1176 个；针对境内网站的仿冒页面数量 2392 个。

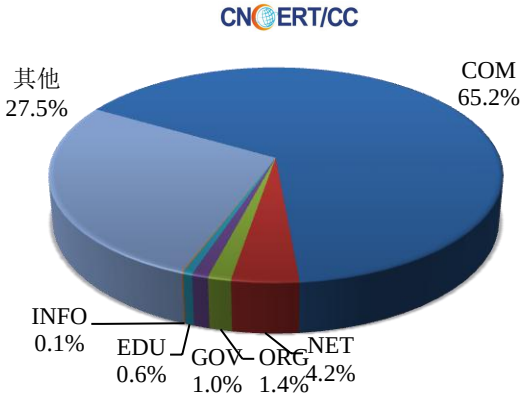


本周境内被篡改政府网站（GOV 类）数量为 18 个（约占境内 0.2%），较上周环比上升 1700.0%；境内被植入后门的政府网站（GOV 类）数量为 12 个（约占境内 1.0%），较上周环比上升 50.0%；针对境内网站的仿冒页面涉及域名 764 个，IP 地址 724 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(5/20-5/26)

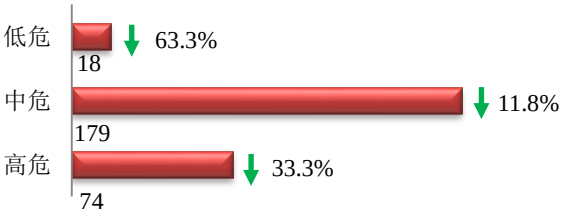


本周我国境内被植入后门网站按类型分布
(5/20-5/26)

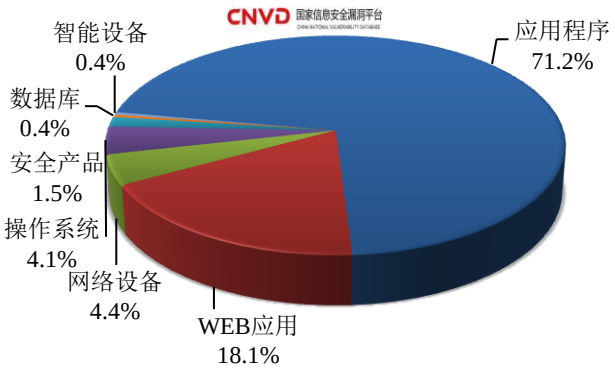


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 271 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
(5/20-5/26)



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 应用漏洞和网络设备漏洞。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

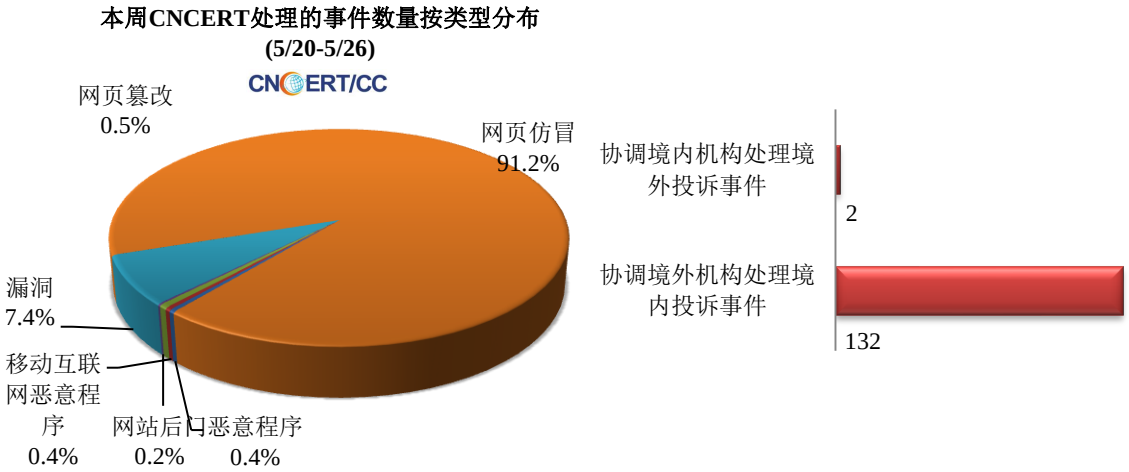
CNVD漏洞周报发布地址

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

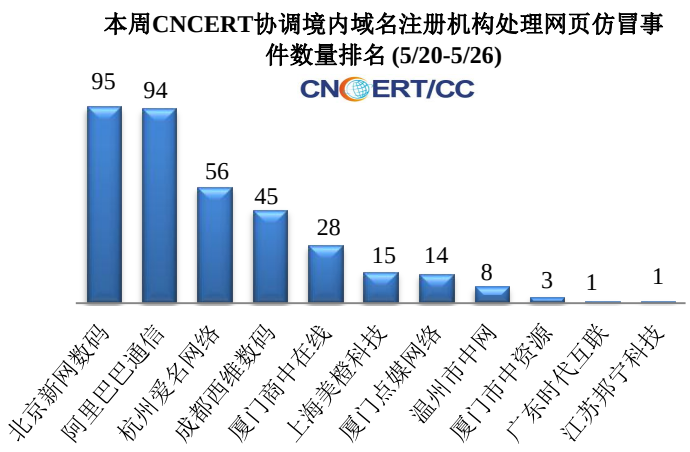
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 556 起，其中跨境网络安全事件 134 起。

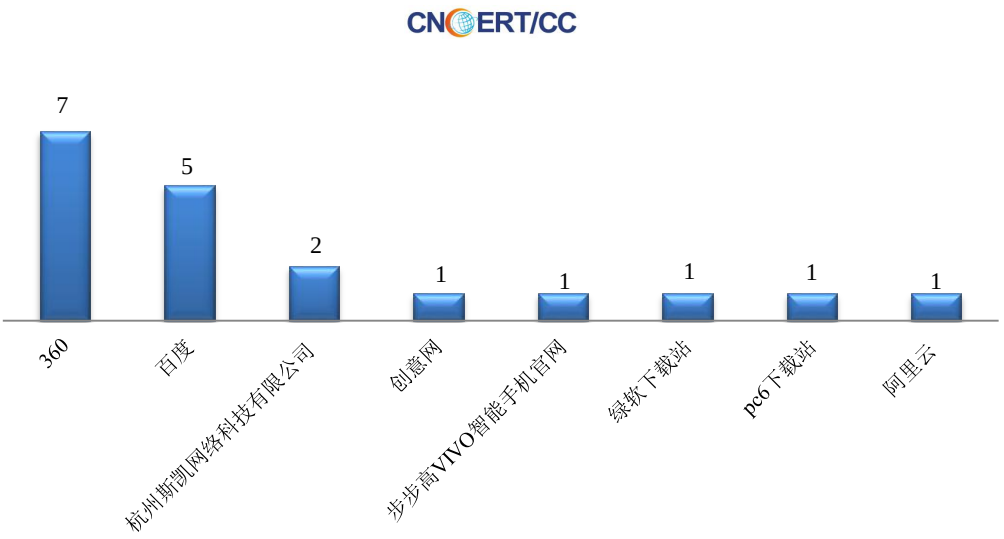


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 507 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 503 起和政府公益事件 2 起。



本周，CNCERT 协调 8 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 (5/20-5/26)



业界新闻速递

1、网信办通报百款常用 App 申请收集个人信息权限情况

新京报 5 月 24 日消息由中央网信办、工信部、公安部、市场监管总局等多部门指导的 App 专项治理工作组，发布了对下载量大的百款 App 申请权限以及强制开启的权限进行的分析统计结果。权限是操作系统内置的访问控制机制。安卓（Android）操作系统通过权限来控制 App 对系统资源和个人信息的访问使用。App 只有在系统层面获取了某项权限，才能执行与该权限有关的操作。

2、黑客使用 NSA 黑客工具攻击美国政府网络

E 安全 5 月 24 日消息 美国马里兰州巴尔的摩市遭受严重的恶意软件攻击，攻击持续了近三周，导致政府电脑、电子邮件无法使用，房地产销售、水费账单等服务中断。永恒之蓝是 NSA（美国国家安全局）开发的最强大的黑客工具之一，黑客如今使用它攻击美国政府网络。黑客曾利用 NSA 的黑客工具，进行了一些破坏性极强的攻击，如 WannaCry、NotPetya 等。永恒之蓝曾入侵了全球数百万个系统，现在它出现在了 NSA 总部所处的城市——巴尔的摩市。该工具利用未安装补丁的系统，允许攻击者获得系统访问权，并使用恶意软件接管网络中的其他系统。.

3、谷歌利用 Gmail 读取网购收据，跟踪用户购买历史

E 安全 5 月 22 日消息 据外媒报道，用户可通过谷歌 Gmail 的“购买”（Purchases）页面访问购买记录，该页面显示了近几年来用户在 Amazon、Flipkart、Swiggy 等在线服务中购买的产品列表。虽然谷歌早已宣布将停止通过 Gmail 收集投放广告的数据，据 CNBC 的报道，谷歌仍在幕后收集大量个人信息。谷歌发言人表示，为了帮助用户在某个地方更方便地查看和跟踪自己购买、预订和订阅的服务，谷歌创建了只有用户个人才能看到的私人目的地。用户可以随时删除此信息。谷歌不会使用 Gmail 邮件中的任何信息为用户提供广告服务，包括在购买页面上显示的电子邮件收据和确认信息。实际上删除这些信息并不容易。由于没有批量删除数据的选项，删除数据并不方便，只能一个一个地删除。许多人习惯于将收据保存在 Gmail 中，以便在以后需要退货时使用。

4、Snapchat 员工滥用内部工具 获取位置数据等信息

新浪财经 5 月 24 日消息 根据美国科技媒体 Motherboard 的报道，Snap 的前员工表示，几年前有“多名”Snap 员工通过不当方式访问用户数据。这意味着他们滥用了自己的权限，在合法理由之外监视用户。Snap 的员工拥有内部工具，让他们可以访问 Snapchat 用户的个人信息，包括位置数据、在应用上保存的照片，以及电子邮件地址。这样的工具之一是 SnapLion，其设计是为了满足司法部门获得用户数据的要求。然而，Snap 的反垃圾邮件团队、客户运营团队和信息安全人员都可以使用该工具。

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：吕志泉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315