国家互联网应急中心

2019 年第 20 期
5 月 13 日-5 月 19 日

网络安全信息与动态周报

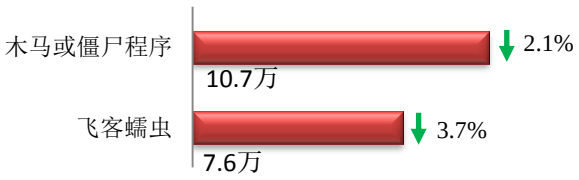
本周网络安全基本态势

境内感染网络病毒的主机数量	• 18.3万	↓ 2.8%
境内被篡改网站总数[1] 其中政府网站数量	• 1474 • 1	↓ 71.6% ↓ 94.1%
境内被植入后门网站总数 其中政府网站数量	• 1077 • 8	↓ 23.5% ↓ 84.3%
针对境内网站的仿冒页面数量	• 1106	↓ 40.3%
新增信息安全漏洞数量 其中高危漏洞数量	• 363 • 111	↑ 31.0% ↑ 42.3%

= 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

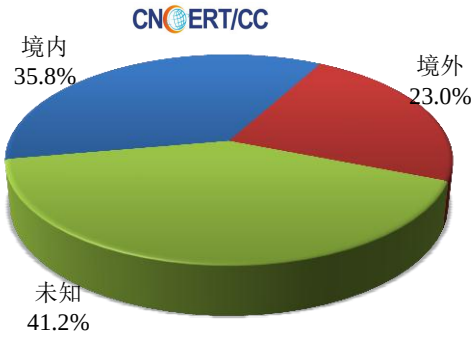
本周境内感染网络病毒的主机数量约为 18.3 万个，其中包括境内被木马或被僵尸程序控制的主机约 10.7 万以及境内感染飞客（conficker）蠕虫的主机约 7.6 万。



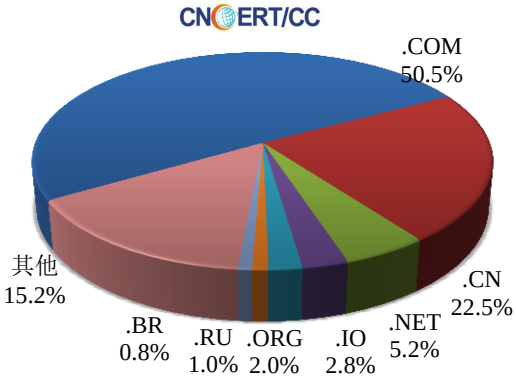
[1]本期境内被篡改网站数量受监测数据范围扩大影响，波动较大

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 3213 个，涉及 IP 地址 5274 个。在 3213 个域名中，有 23.0%为境外注册，且顶级域为.com 的约占 50.5%；在 3213 个 IP 中，有约 52.6%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 588 个 IP。

本周放马站点域名注册所属境内外分布
(5/13-5/19)



本周放马站点域名所属顶级域的分布
(5/13-5/19)



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。

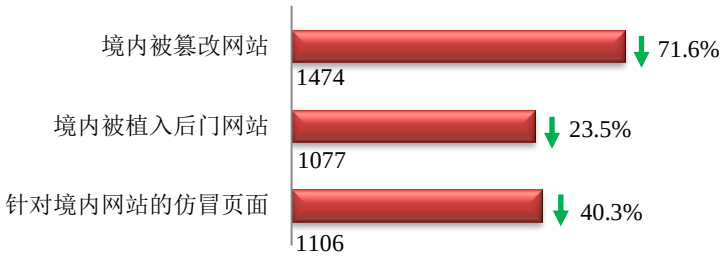
ANVA恶意地址黑名单发布地址

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。

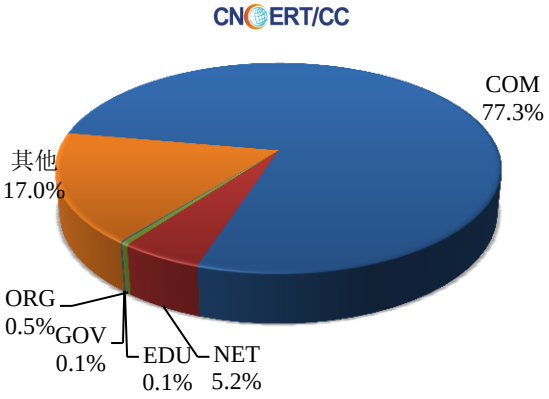
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 1474 个；境内被植入后门的网站数量为 1077 个；针对境内网站的仿冒页面数量 1106 个。

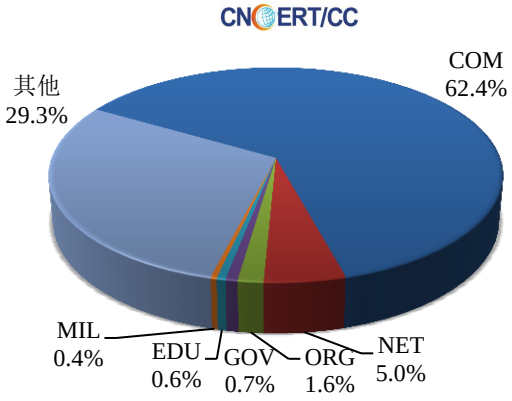


本周境内被篡改政府网站（GOV 类）数量为 1 个（约占境内 0.1%），较上周环比下降 94.1%；境内被植入后门的政府网站（GOV 类）数量为 8 个（约占境内 0.7%），较上周环比下降 84.3%；针对境内网站的仿冒页面涉及域名 490 个，IP 地址 229 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(5/13-5/19)

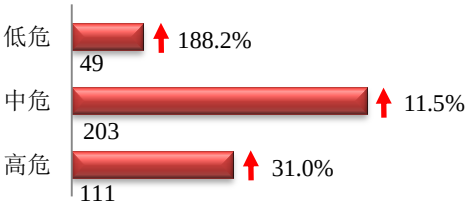


本周我国境内被植入后门网站按类型分布
(5/13-5/19)

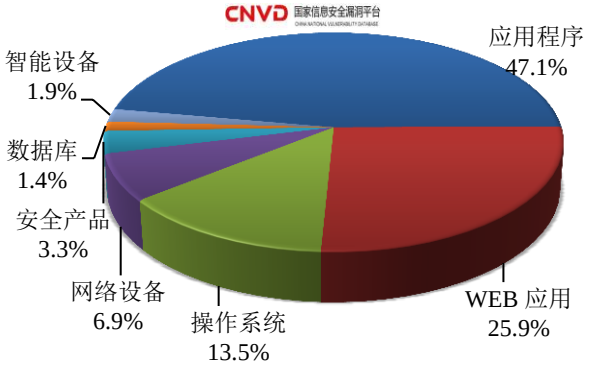


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 363 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
(5/13-5/19)



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。

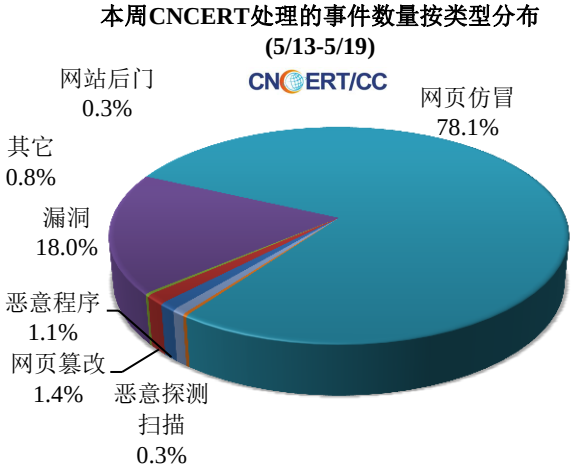
CNVD漏洞周报发布地址

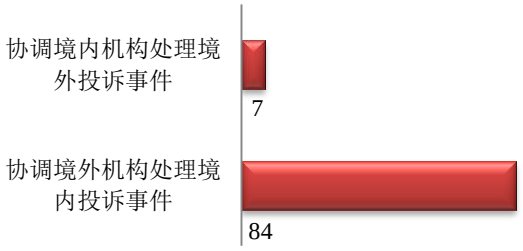
http://www.cnvd.org.cn/webinfo/list?type=4

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。

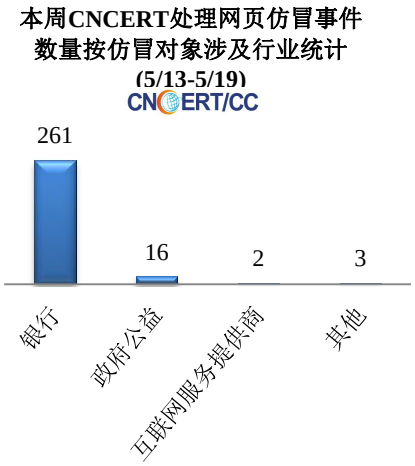
本周事件处理情况

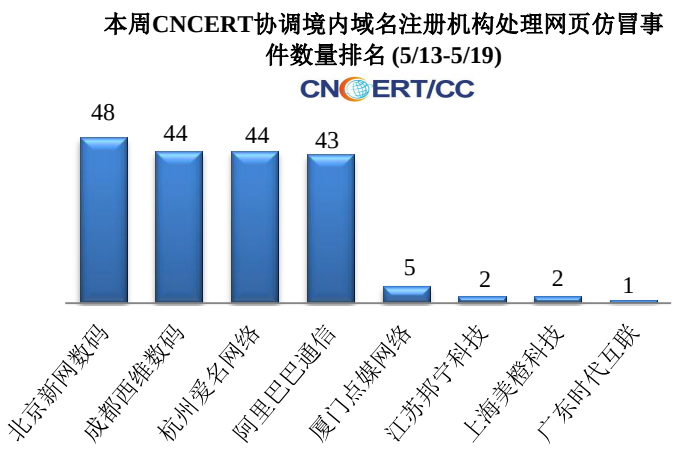
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 361 起，其中跨境网络安全事件 91 起。





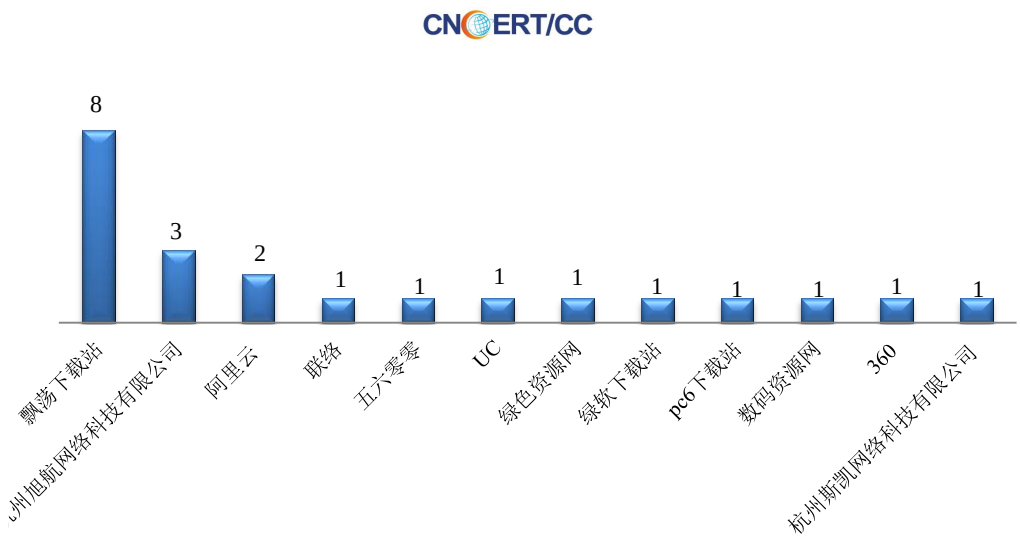
本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 282 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 261 起和政府公益事件 16 起。





本周，CNCERT 协调 12 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 22 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
(5/13-5/19)



业界新闻速递

1、网络安全等级保护制度 2.0 国家标准宣贯会成功召开

搜狐新闻 5 月 16 日消息 网络安全等级保护制度 2.0 国家标准宣贯会在北京隆重召开并取得圆满成功。公安部网络安全保卫局、国家市场监管总局、重要行业部门、企事业单位的领导嘉宾，以及测评机构和安全建设整改机构的技术负责人、互联网企业代表等近千人参加宣贯会。 本次宣贯会由公安部网络安全保卫局指导，公安部第三研究所和公安部第一研究所共同主办。等级保护制度 2.0 国家标准的发布，是具有里程碑意义的一件大事，标志着国家网络安全等级保护工作步入新时代，对保障和促进国家信息化发展，提升国家网络安全保护能力，维护国家保护空间安全具有重要的意义。

2、伊朗成立特别工作组应对美国的网络威胁

E 安全 5 月 15 日消息 伊朗通信和信息技术部部长表示，部门已经组织了一个特别工作组来应对美国的网络威胁。通信和信息技术部已制定了多项举措，以应对美国政府的网络恐怖主义行为和敌对措施。美国对伊朗网络行业的大部分制裁是在过去一年实施的。尽管所有国际云计算提供商已停止向伊朗企业提供互联网服务，但伊朗的网络空间并未受到干扰。伊朗已经制定了必要的计划来解决可能的互联网断网问题。

3、俄罗斯多个政府网站共泄露 225 万用户隐私

安全内参 5 月 16 日消息,俄罗斯多个政府网站泄露了超过 225 万公民、政府雇员和高级官员的个人和护照信息。俄罗斯非政府组织 information Culture 的联合创始人发现了本次泄露事件，并调查了政府在线认证中心和

50 个政府门户网站，发现其中 23 个网站泄露了个人保险账号，14 个网站泄露了护照信息。网站负责人员将此次泄露归咎于政府文档管理操作不当、IT 人员技术水平较低以及内部监控设施不够完善。

4、“三只小猫”漏洞威胁全球数百万思科路由器

cnBeta.COM5 月 15 日消息 美国安全研究公司近日发布了一份报告，公布了思科产品的两个漏洞。第一个漏洞被称为三只小猫（Thrangrycat），允许攻击者通过现场可编程门阵列（FPGA）比特流操作完全绕过思科的信任锚模块（TAm）。第二个是针对 Cisco IOS XE 版本 16 的远程命令注入漏洞，该漏洞允许以 root 身份执行远程代码，通过链接三只小猫和远程命令注入漏洞，攻击者可以远程持续绕过思科的安全启动机制，并锁定 TAm 的所有未来软件更新。三只小猫是由 Cisco Trust Anchor 模块中的一系列硬件设计缺陷引起的，Cisco Trust Anchor 模块（TAm，信任锚）于 2013 年首次商业化推出，是一种专有的硬件安全模块，用于各种思科产品，包括企业路由器，交换机和防火墙。TAm 是专门用来验证安全开机程序的硬件装置，在系统开启时执行一连串的指令，以立即验证开机载入程序的完整性，一但侦测到任何不妥，就会通知使用者并重新开机，以防止设备执行被窜改的开机载入程序。三只小猫可藉由操纵 FPGA（Field Programmable Gate Array，现场可编程门阵列）的比特流（bitstream）来绕过 TAm 的保护。

5、优衣库信息被泄露 优衣库公司声明：不涉中国网站

E 安全 5 月 15 日消息 日本迅销公司发布声明说，旗下品牌优衣库、GU 销售网站逾 46 万名客户个人消息遭未授权访问，可能造成信息泄露。共同社援引声明内容报道，优衣库和 GU 两家线上店 4 月 23 日和 5 月 10 日遭黑客攻击，客户姓名、地址、电话号码和信用卡信息可能泄露。不过，目前还没有相关信息为第三方使用的报告。

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：张帅

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315