国家互联网应急中心

网络安全信息与动态周报

2018 年第 20 期

5 月 14 日-5 月 20 日

CNCERT/CC

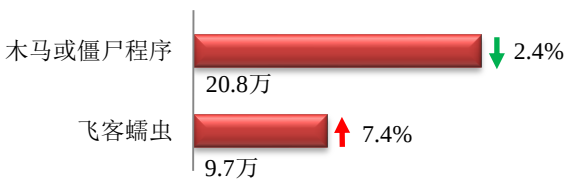
本周网络安全基本态势

境内感染网络病毒的主机数量	•30.5万	0.5%
境内被篡改网站总数 其中政府网站数量	•956 •32	12.5% 3.0%
境内被植入后门网站总数 其中政府网站数量	•922 •25	2.1% 10.7%
针对境内网站的仿冒页面数量	•750	47.6%
新增信息安全漏洞数量 其中高危漏洞数量	•353 •149	35.8% 140.3%

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*

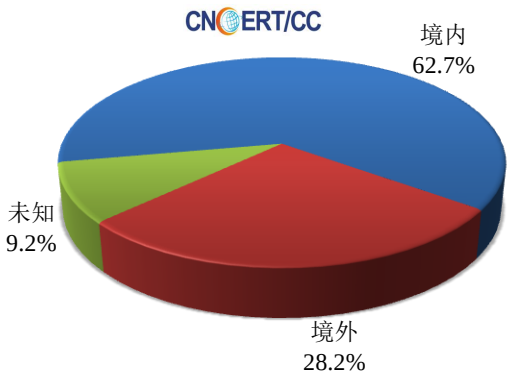
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 30.5 万个，其中包括境内被木马或被僵尸程序控制的主机约 20.8 万以及境内感染飞客（conficker）蠕虫的主机约 9.7 万。

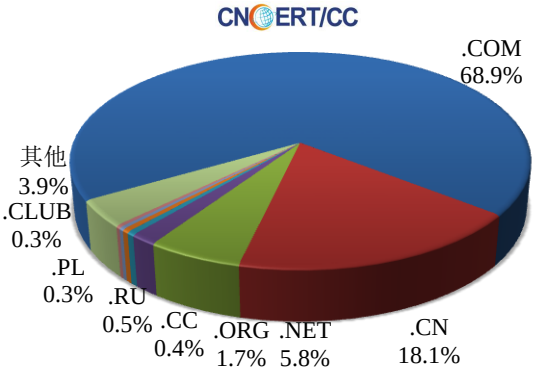


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 1562 个，涉及 IP 地址 117756 个。在 1562 个域名中，有 28.2%为境外注册，且顶级域为.com 的约占 68.9%；在 117756 个 IP 中，有约 36.5%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 325 个 IP。

本周放马站点域名注册所属境内外分布
(5/14-5/20)



本周放马站点域名所属顶级域的分布
(5/14-5/20)



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。

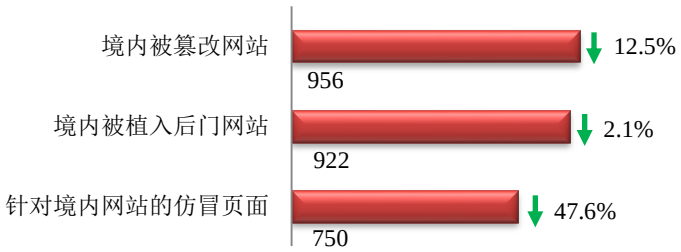
ANVA恶意地址黑名单发布地址

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。

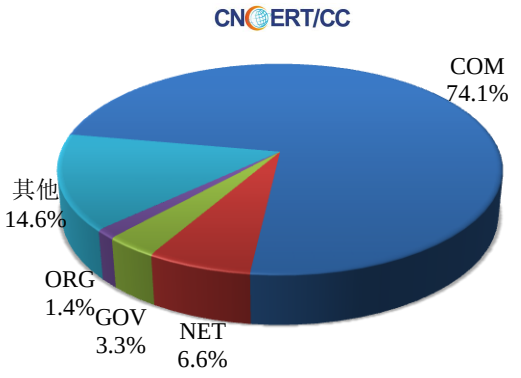
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 956 个；境内被植入后门的网站数量为 922 个；针对境内网站的仿冒页面数量为 750。

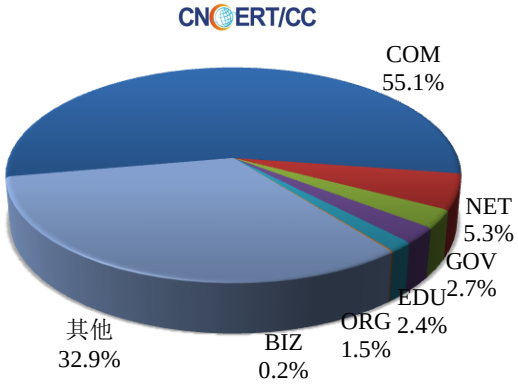


本周境内被篡改政府网站（GOV 类）数量为 32 个（约占境内 3.3%），较上周环比下降了 3.0%；境内被植入后门的政府网站（GOV 类）数量为 25 个（约占境内 2.7%），较上周环比下降了 10.7%；针对境内网站的仿冒页面涉及域名 293 个，IP 地址 160 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(5/14-5/20)

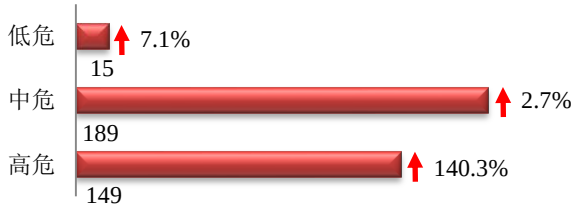


本周我国境内被植入后门网站按类型分布
(5/14-5/20)

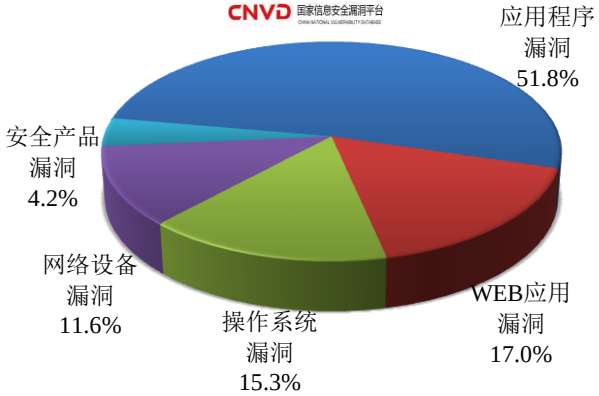


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 353 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
(5/14-5/20)



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

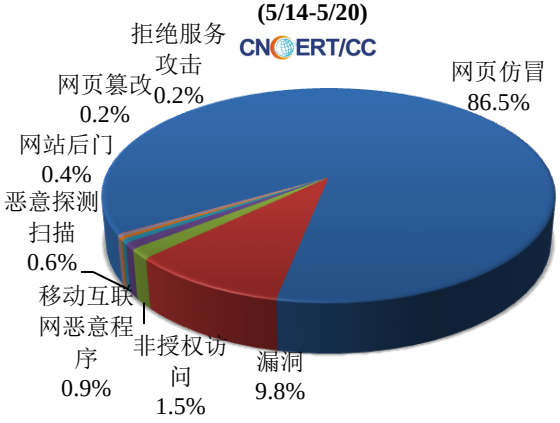
http://www.cnvd.org.cn/webinfo/list?type=4

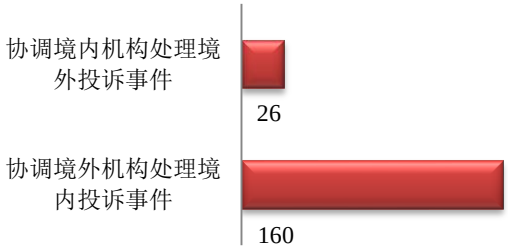
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 533 起，其中跨境网络安全事件 186 起。

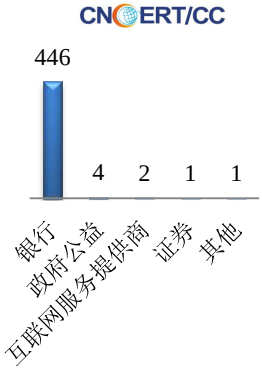
本周CNCERT处理的事件数量按类型分布 (5/14-5/20)



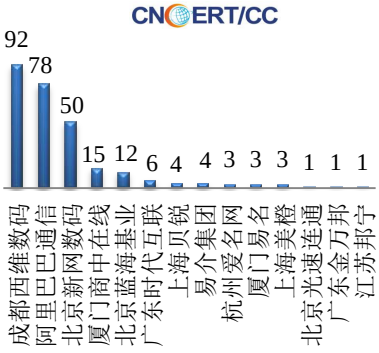


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 454 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 446 起和政府公益仿冒事件 4 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(5/14-5/20)

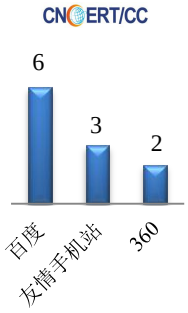


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (5/14-5/20)



本周，CNCERT 协调 3 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 11 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
(5/14-5/20)



业界新闻速递

1、中德高级别安全对话框架下的网络安全磋商在京举行

中新网 5 月 18 日消息 5 月 17 日下午，公安部副部长侍俊与德国联邦内政部国务秘书京特·克林斯在北京共同主持中德高级别安全对话框架下的网络安全磋商。双方秉持平等互信、坦诚务实的态度，就网络犯罪形势、网络犯罪和安全领域相关立法情况、打击网络犯罪、打击网络恐怖主义等进行了交流，并就下一步加强网络安全执法合作进行了深入探讨。双方同意，在中德高级别安全对话机制框架下，共同推进两国执法部门在网络安全领域的合作。

2、美国国土安全部发布《网络安全战略》

E 安全 5 月 17 日消息 2018 年 5 月 15 日，美国国土安全部发布网络安全战略，希望更积极地履行网络安全使命，以保护关键基础设施免于遭受网络攻击。该战略旨在使美国国土安全部的网络安全工作规划、设计、预算制定和运营活动按照优先级协调开展。该战略将致力于协调各部门的网络安全活动，以确保相关工作的协调一致。该战略确定了美国国土安全部管理网络安全风险的五大主要方向，包括风险识别、减少关键基础设施脆弱性、降低网络犯罪活动威胁、缓解网络事件影响、实现网络安全成果，以及 7 个明确目标，包括：评估不断变化的网络安全风险、保护美国联邦政府信息系统、保护关键基础设施、防止并打击网络空间的犯罪活动、有效响应网络事件、提高网络生态系统的安全性和可靠性、加强管理美国国土安全部网络安全活动。

3、白宫取消网络安全协调员职位

新华网 5 月 17 日消息 2018 年 5 月 15 日，美国国家安全委员会证实，由总统唐纳德·特朗普任命的首名网络安全协调官上周辞职后，白宫决定不再设立这一职位。网络安全协调官一职由前任总统贝拉克·奥巴马设立，以协调政府网络安全和数字战争政策。委员会发言人罗伯特·帕拉迪诺在一份声明中说，这一决定意在“赋

予国家安全委员会高级主管更多权力”,“精简管理层有助于提高效率、简化官僚体系并加强问责”,网络安全协调官职位取消后，国家安全委员会两名高级网络政策主管将实时协调事务。

4、卢森堡发布新版网络安全战略

E 安全 5 月 15 日消息 2018 年 5 月 8 日，卢森堡副总理 Xavier Bettel 和国家保护高级专员 Luc Feller 共同发布了该国的第三版网络安全战略。该战略旨在反映欧盟委员会制定的国家层面的一揽子计划的目标，同时也反映了日益数字化的世界，由 Luc Feller 所领导的特别工作组制定。根据卢森堡的“数字卢森堡”倡议，该战略将致力于通过加强识别网络攻击和保护数字基础设施的能力以及提高利益相关方的防御意识等措施，增强公众对数字环境的信心和加强信息系统的安全性。该战略以 “建立公众对数字环境的信任，保护数字基础设施和促进经济发展”为指导思想。各指导思想明确了目标：建立对数字环境的信任；保护数字基础设施；促进经济。

5、丹麦铁路运营商 DSB 遭遇 DDoS 攻击，多系统受影响

E 安全 5 月 16 日消息 2018 年 5 月 14 日，丹麦铁路运营商 DSB 证实其于 5 月 13 日遭遇了大规模的 DDoS 攻击，事件造成约 1.5 万客户旅客无法通过该公司的应用程序、售票机、网站和商店购买火车票，运营商只得人工售票，问题在 5 月 14 日上午得到解决。丹麦铁路运营商 DSB 每年输送的旅客超过 1.95 亿，该运营商负责运营丹麦铁路的大多数旅客列车及铁路维护服务。DSB 副主任阿斯克·维特·克努森表示，DSB 的技术人员和 IT 承包商经过仔细分析得出的结论是：这是一场外部攻击，有人企图关闭 DSB 的系统。另据丹麦当地媒体 The Local 报道，这起攻击还影响了 DSB 的内部邮件和电话系统，导致 DSB 不得不选择通过社交媒体进行通信。

6、墨西哥多家银行巨款神秘消失 或遭“黑客”窃取

新华网 5 月 16 日消息 墨西哥中央银行和监管机构 14 日说，1800 万至 2000 万美元近期在多家银行的电子转账过程中不翼而飞，可能遭“黑客”窃取。中央银行企业支付和服务系统主管洛伦扎·马丁内斯说，4 月到 5 月至少发生 5 起针对墨西哥官方电子支付系统 SPEI 的袭击。遗失金额可能在 3.5 亿至 4 亿比索（1875 万至 2039 万美元）之间。部分款项通过 SPEI 系统转账，交易者身份和收款人信息暂时不清楚。在墨西哥，跨行支付系统允许不同银行之间实时转账。一名消息人士说，黑客可能在银行有内应，缘由是如此大量现金提取在墨西哥并不常见。据美联社报道，三家银行 4 月 27 日在软件筛查过程中发现漏洞，其他银行继而马上进入安全检测模式，发现巨款“窟窿”。马丁内斯说，SPEI 系统没有受到破坏，但由其他机构或第三方提供的连接支付系统的软件出现漏洞。中央银行要求所有银行追加安全举措，延长借记卡消费预授权、电子支付等交易的转账时间。这对一些零售银行业务客户或自助柜员机（ATM）用户而言无疑会带来一定的不便。

7、Facebook 曝 300 万用户数据泄露

cnBeta.COM5 月 15 日消息 2018 年 5 月 15 日，美国媒体 New Scientist 报道称，有研究者在 Facebook 平台上开发了性格测试应用 myPersonality，但将用户反馈的答案保存在不安全的网站上。这可能导致多达 300 万用户的信息泄露。尽管这并不像“剑桥分析”数据泄露事件一样严重，但存在一定关联。这些数据的所有者是剑桥大学心理计量学中心的研究者，而“剑桥分析”丑闻的核心人物亚历山大·科根（Alexander Kogan）也参与了该项目。共有 600 万用户参与了这款应用的测试，其中一半的人同意分享自己的答案和数据。然而，剑桥

大学心理计量学中心通过不安全的网站向数百名研究者分发这些数据。答案中还包括年龄、性别、所在地点和状态更新等信息，而这些信息均关联至唯一识别符，导致用户的个人情况更容易暴露。此外，尽管按照规则只有学术研究者可以访问这些数据，但过去 4 年中，任何人都可以在网上搜索到相关的用户名和密码，以访问这些数据。Facebook 已证实于 4 月 7 日暂停了这款应用，原因是这款应用将用户数据传输给他人。此外根据进一步调查的结果，Facebook 可能会永久封禁这款应用。

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：陈阳

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158