国家互联网应急中心

网络安全信息与动态周报

2020 年第 20 期

5 月 11 日-5 月 17 日

CNCERT/CC

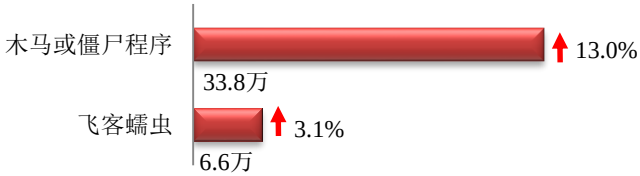
本周网络安全基本态势

境内感染网络病毒的主机数量	•40.4万	↑ 11.3%
境内被篡改网站总数 其中政府网站数量	•7361 •41	↑ 0.03% ↑ 32.3%
境内被植入后门网站总数 其中政府网站数量	•1678 •3	↓ 6.5% ↓ 50.0%
针对境内网站的仿冒页面数量	•826	↑ 31.3%
新增信息安全漏洞数量 其中高危漏洞数量	•336 •115	↓ 53.0% ↓ 65.3%

= 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

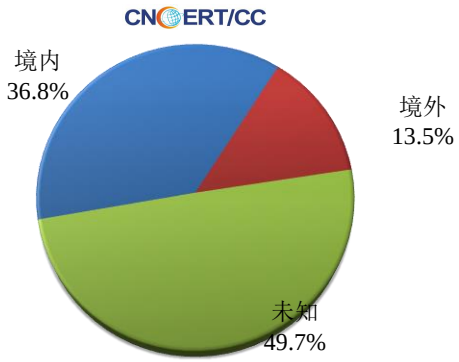
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 40.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 33.8 万以及境内感染飞客（conficker）蠕虫的主机约 6.6 万。

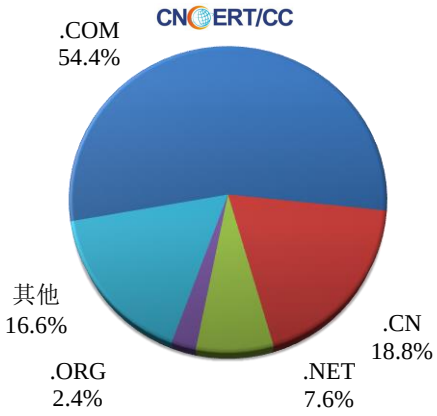


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 902 个，涉及 IP 地址 4294 个。在 902 个域名中，有 13.5%为境外注册，且顶级域为.com 的约占 54.4%；在 4294 个 IP 中，有约 54.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 340 个 IP。

本周放马站点域名注册所属境内外分布
(5/11-5/17)



本周放马站点域名所属顶级域的分布
(5/11-5/17)



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。

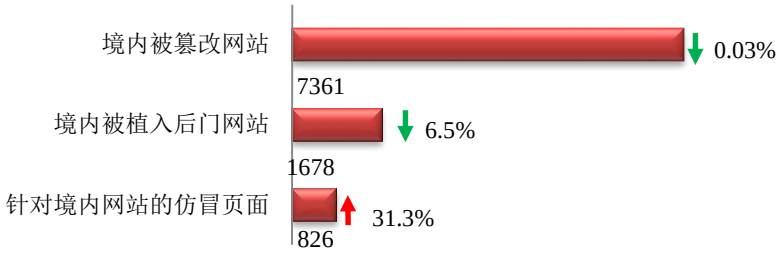
ANVA恶意地址黑名单发布地址

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。

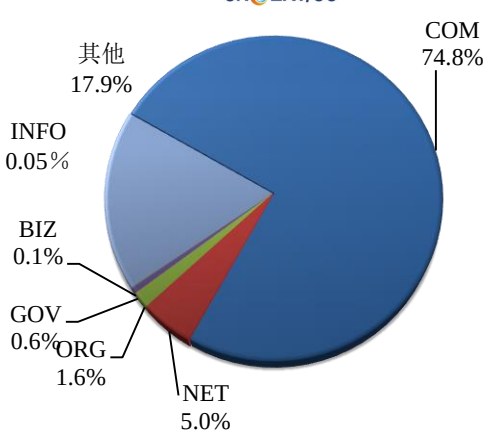
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 7361 个；被植入后门的网站数量为 1678 个；针对境内网站的仿冒页面数量 826 个。

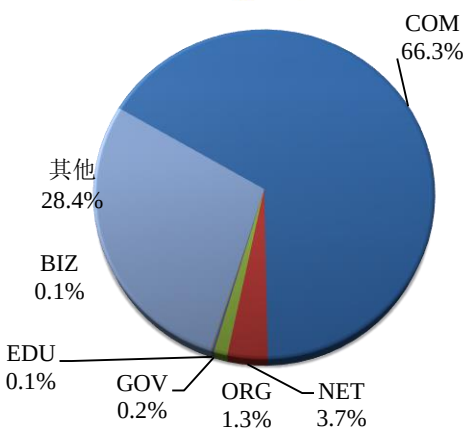


本周境内被篡改政府网站（GOV 类）数量为 41 个（约占境内 0.6%），较上周上涨了 32.3%；境内被植入后门的政府网站（GOV 类）数量为 3 个（约占境内 0.2%），较上周下降了 50.0%。

本周我国境内篡改网站按类型分布
(5/11-5/17)

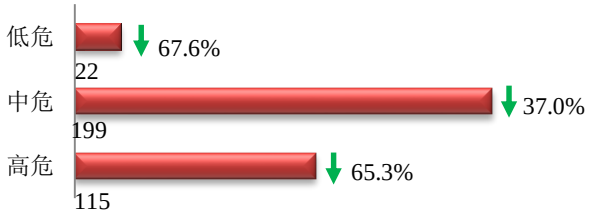


本周我国境内被植入后门网站按类型分类
(5/11-5/17)

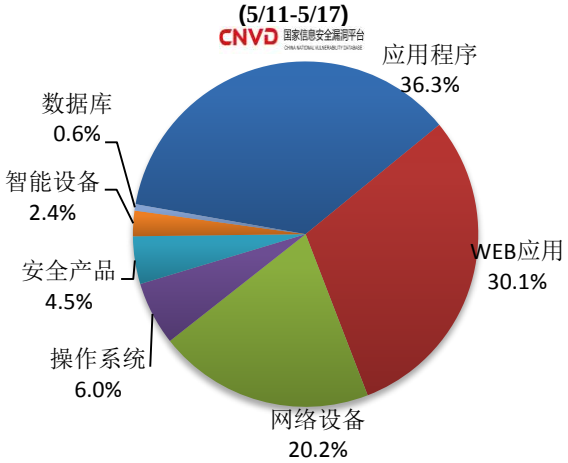


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 336 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分布
(5/11-5/17)



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 应用和网络设备。

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

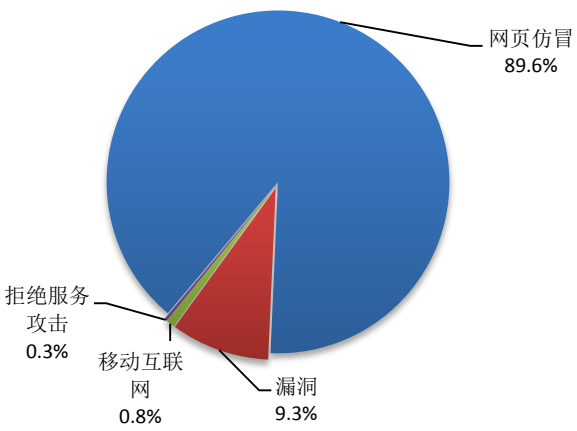
http://www.cnvd.org.cn/webinfo/list?type=4

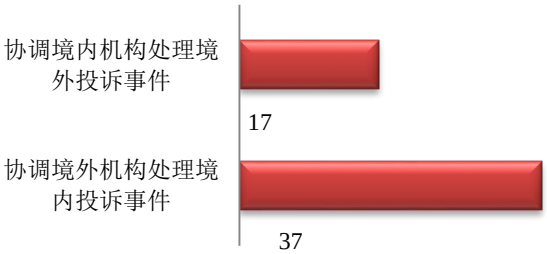
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 365 起，其中跨境网络安全事件 54 起。

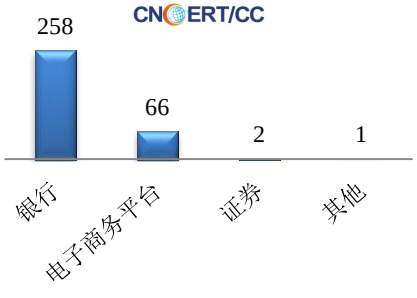
本周CNCERT处理的事件数量按类型分布
(5/11-5/17)



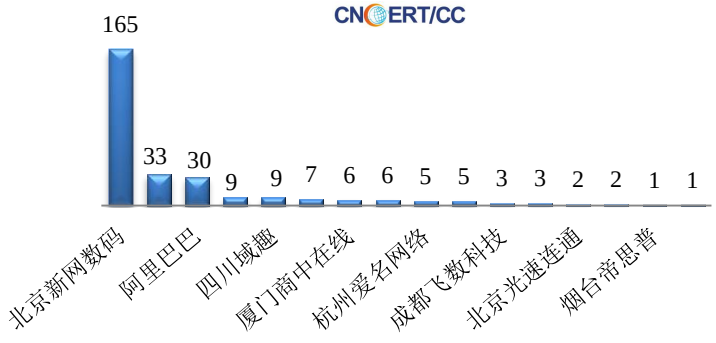


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 327 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 258 起、电子商务平台 66 起和证券仿冒事件 2 起和其他事件 1 起。

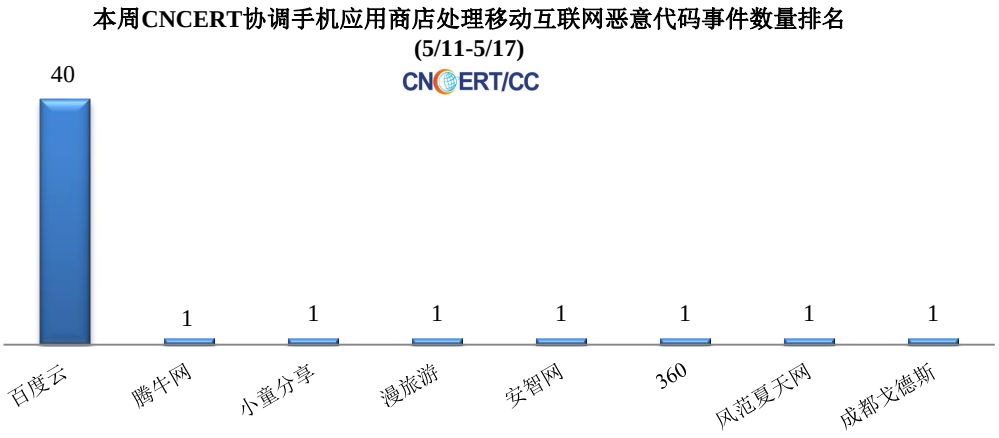
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计
(5/11-5/17)



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 (5/11-5/17)



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 47 个。



业界新闻速递

1、 工信部印发《关于工业大数据发展的指导意见》

5 月 13 日，工业和信息化部印发《关于工业大数据发展的指导意见》（工信部信发〔2020〕67 号），明确将促进工业数据汇聚共享、深化数据融合创新、提升数据治理能力、加强数据安全管理，着力打造资源富集、应用繁荣、产业进步、治理有序的工业大数据生态体系，并提出加快数据汇聚、推动数据共享、深化数据应用、完善数据治理、强化数据安全、促进产业发展、加强组织保障等七方面 21 条指导意见。

2、 微软发布了五月份补丁更新 共修复安全漏洞 111 个

5 月 12 日，微软发布了五月份安全更新共修复了 111 个漏洞，其中 13 个为严重漏洞，91 个为重要漏洞，3 个为中危险漏洞，4 个低危险漏洞，无 0day 漏洞或未修补的漏洞。其中，Microsoft Edge 存在的 3 个严重漏洞：Microsoft Edge 特权提升漏洞（CVE-2020-1056）、Microsoft Edge 欺骗漏洞（CVE-2020-1059）、Microsoft Edge PDF 远程执行代码漏洞（CVE-2020-1096）和色彩管理模块（ICM32.dll）存在 1 个严重漏洞（CVE-2020-1117）允许攻击者通过诱骗用户访问恶意网站来进行远程代码执行。

3、 Google Firebase 错误配置使 4000 个 Android App 数据遭泄露

5 月 15 日，据外媒报道，由于 Google Firebase 发生严重错误配置，导致 4000 个 Android app 的用户数据遭泄露。目前，在 Google Play 商店中，有超过 30％的应用都在

使用 Firebase 服务。Firebase 的错误配置允许任何人无需密码或任何其他身份验证即可访问包含用户个人信息、访问令牌和其他信息的数据库。根据研究人员的统计，发现配置错误的应用程序已经被 Android 用户安装了 42.2 亿次，同时使用这些应用可能会给用户隐私带来巨大的风险。研究人员发现的一些被公开数据中包含 700 多万条电子邮件地址、440 万个用户名信息、100 多万条帐号密码信息、530 多万的用户电话号码以及其他重要的用户居住定位信息和 GPS 数据。目前，Google 已经向开发人员发送了有关其部署中可能存在的错误配置的通知，并提供了纠正建议。

4、 微软分享了 COVID-19 网络攻击威胁的签名数据

5 月 16 日，cnBeat 网站消息，微已决定分享与 COVID-19 网络攻击相关的威胁签名数据。为保护企业和个人用户免受威胁，微软汇总了跨云端、个人节点、应用程序和电子邮件的无数线索信号。作为一个开源项目，这份签名数据旨在帮助全行业提升识别和应对此类攻击的能力。微软威胁情报团队希望提升应对威胁的透明度和造福更广泛的安全社区，并呼吁更多企业参与其中，大家共同努力帮保护客户和防范趁着 COVID-19 疫病搞发起网络攻击恶意行为者。据悉，开发者可通过 Azure Sentinel GitHub 和 Microsoft Graph Security API 来访问分享的数据。那些使用 MISP 存储威胁数据的企业，还可灵活使用 MISP feed 。

5、 欧洲多国超级计算机集群感染挖矿恶意软件

5 月 16 日，据外媒报道，近日英国、德国、瑞士和西班牙等国超级计算机中心纷纷报告被加密货币恶意软件感染，导致多个高性能计算集群关闭。研究人员对恶意样本进行了分析，肆虐欧洲超级计算机的挖矿恶意软件攻击来自同一个攻击者，该攻击者获得对超级计算节点的访问权限后，就利用 CVE-2019-15666 漏洞进行了根访问，然后部署了挖掘 Monero（XMR）加密货币的应用程序。

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 2019 年，CNCERT 已与 78 个国家和地区的 260 个组织建立了“CNCERT 国际合作伙伴”关系。CNCERT 还积极参加亚太经合组织、国际电联、上合组织、东盟、金砖等政府层面国际和区域组织的网络安全相关工作。

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：贾世琳

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315