国家互联网应急中心

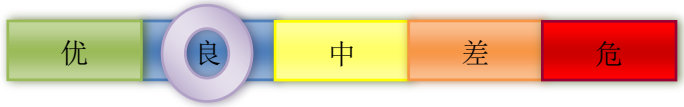
2018 年第 18 期

4 月 30 日-5 月 6 日

网络安全信息与动态周报

CNCERT/CC

本周网络安全基本态势

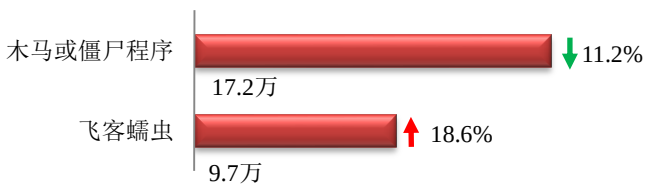


境内感染网络病毒的主机数量	•26.9万	↓ 2.4%
境内被篡改网站总数 其中政府网站数量	•1040 •35	↑ 6.3% ↑ 52.2%
境内被植入后门网站总数 其中政府网站数量	•831 •21	↓ 20.6% ↑ 16.7%
针对境内网站的仿冒页面数量	•1579	↑ 92.3%
新增信息安全漏洞数量 其中高危漏洞数量	•244 •79	↓ 39.0% ↓ 41.9%

═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

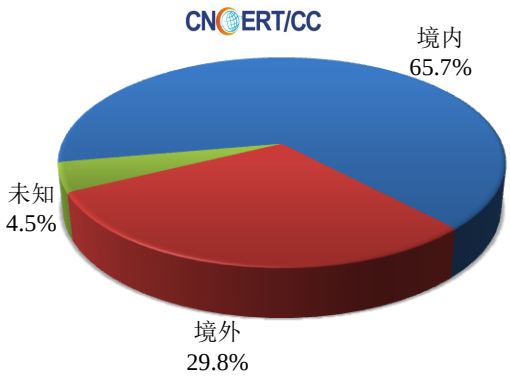
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 26.9 万个，其中包括境内被木马或被僵尸程序控制的主机约 17.2 万以及境内感染飞客（conficker）蠕虫的主机约 9.7 万。

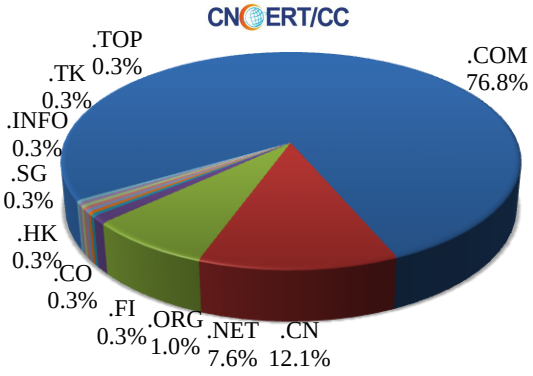


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 289 个，涉及 IP 地址 8265 个。在 289 个域名中，有 29.8%为境外注册，且顶级域为.com 的约占 76.8%；在 8265 个 IP 中，有约 68.1%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 301 个 IP。

本周放马站点域名注册所属境内外分布
(4/30-5/6)



本周放马站点域名所属顶级域的分布
(4/30-5/6)



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。

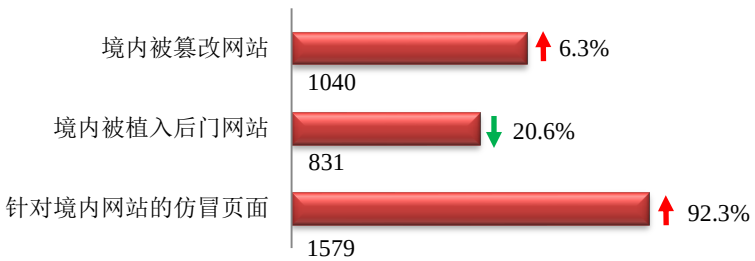
ANVA恶意地址黑名单发布地址

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。

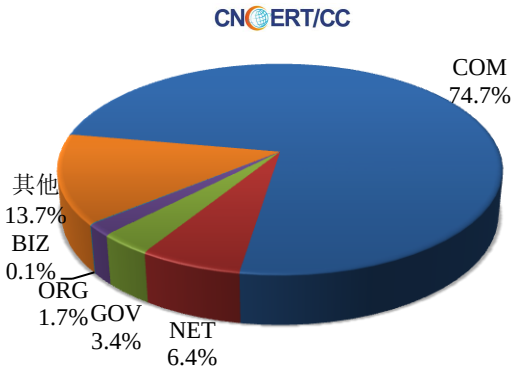
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1040 个；境内被植入后门的网站数量为 831 个；针对境内网站的仿冒页面数量为 1579。

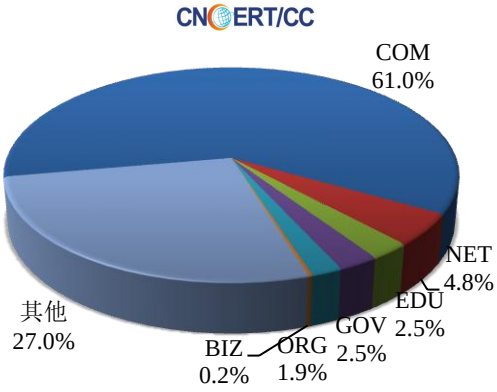


本周境内被篡改政府网站（GOV 类）数量为 35 个（约占境内 3.4%），较上周环比上升了 52.2%；境内被植入后门的政府网站（GOV 类）数量为 21 个（约占境内 2.5%），较上周环比上升了 16.7%；针对境内网站的仿冒页面涉及域名 337 个，IP 地址 181 个，平均每个 IP 地址承载了约 9 个仿冒页面。

本周我国境内被篡改网站按类型分布
(4/30-5/6)

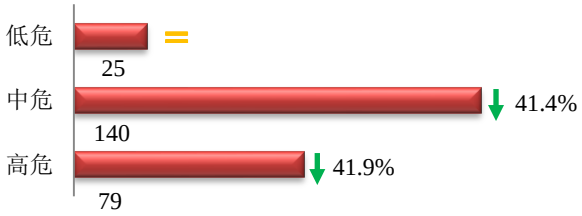


本周我国境内被植入后门网站按类型分布
(4/30-5/6)

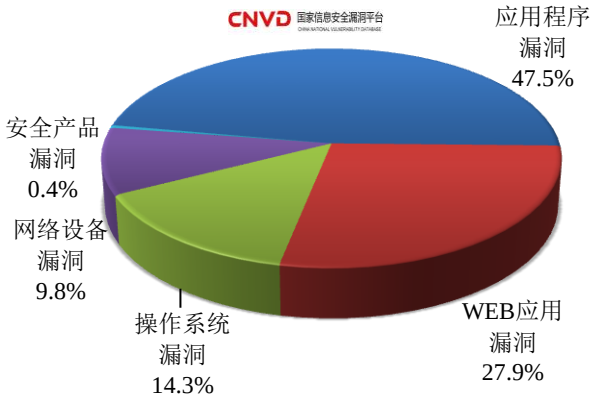


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 244 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
(4/30-5/6)



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

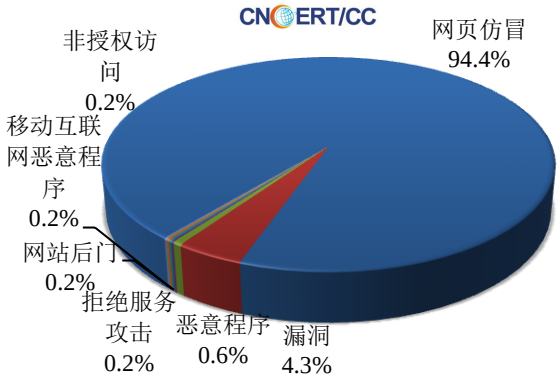
http://www.cnvd.org.cn/webinfo/list?type=4

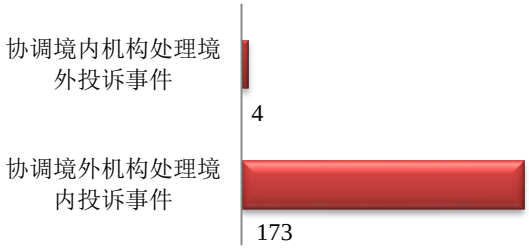
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 514 起，其中跨境网络安全事件 177 起。

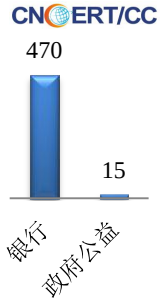
本周CNCERT处理的事件数量按类型分布 (4/30-5/6)



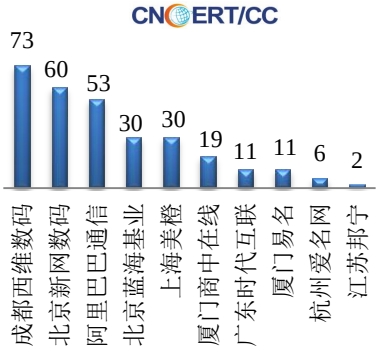


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 485 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 470 起和政府公益仿冒事件 15 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(4/30-5/6)

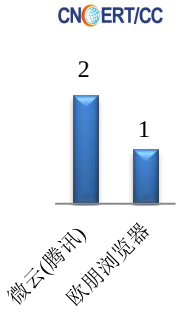


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (4/30-5/6)



本周，CNCERT 协调 2 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 3 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
(4/30-5/6)



业界新闻速递

1、美国对乌克兰的网络防备援助提高到 1000 万美元

E 安全 5 月 5 日消息 根据该部门发言人指出，美国国务院计划将 2017 年向乌克兰承诺的网络防御援助增加一倍，即 1000 万美元，旨在增强各盟友抵御俄罗斯黑客攻击活动的能力。美国国务院发言人希瑟·诺厄特表示，欧洲与欧亚事务国务卿韦斯·米切尔已经于 2018 年 5 月 3 日会见乌克兰总统佩特罗·波罗申科时正式公布了这一消息，目前尚不知道这笔资金将用到何处。美、乌两国 2017 年 9 月曾在基辅（乌克兰首都）进行了首次双边网络安全对话，美国宣布提供 500 万美元网络安全援助，旨在“加强乌克兰预防、缓解及应对网络攻击活动的能力”。2018 年 2 月，美国众议院通过了一项方案，要求国务院提供一切必要的支持以保护乌克兰政府所使用的计算机设备，特别是保护乌克兰关键基础设施的网络体系。美国陆军亦制定乌克兰安全援助计划，希望在乌克兰国防部建立一座复杂的网络作战中心，从而提升乌克兰军事网络的弹性水平。

2、日本政府筹备拥有反网络战能力

新浪网 5 月 4 日消息 日本《读卖新闻》5 月 3 日报道称，日本政府正在协调让自卫队具备反击网络攻击的能力。反击的对象将只限于同时遭受常规武器等物理攻击的情况。最有可能的方案是向作为敌方攻击据点的服务器发送大量数据以致其瘫痪的“分布式拒绝服务攻击（DDoS）”。政府考虑将该方案写入今年末修订的《防卫计划大纲》。政府在《中期防卫力整备计划》（2014 至 2018 财年）中就网络攻击能力写道，“将拥有阻碍对方利用网络空间的能力之可能性纳入视野”，并就可否拥有该能力进行了研究讨论。最终的判断是，针对被认定为“基于国家意志对我国有组织有计划行使武力”的网络攻击的反击能力，与专守防卫的原则不矛盾。政府准备利用修改防卫大纲之机，除了拥有网络反击能力外，还要强化提高网络空间防御能力的对策。目前正在考虑增加人员、与民间企业合作以及有效利用人工智能（AI）等。

3、欧洲央行发布 TIBER-EU 框架以测试金融企业网络弹性

E 安全 5 月 4 日消息 欧洲中央银行（简称欧洲央行）2018 年 5 月 2 日表示，已经设计了一个针对银行、证券交易所和其它金融公司的网络攻击模拟测试。欧洲央行此举旨在创建“欧洲基于威胁情报的道德红队的框架”（简称 TIBER-EU），以测试欧盟金融机构的网络弹性。TIBER-EU 框架是欧洲首个针对可控网络黑客行为的框架，可在多个当局监督的情况下测试跨境实体的网络弹性。除了其它工具，该框架还希望外聘专家充当“红队”，负责发现并利用测试参与公司的漏洞。TIBER-EU 框架将作为一份指南，供其它机构进行任意测试。欧洲央行表示，相关机构和实体可自行决定是否及何时进行基于 TIBER-EU 的测试。测试可量身定制，将会为参与测试的实体了解优势和劣势，并使其通过学习提高网络成熟度。

4、澳大利亚联邦银行遗失 1200 万条用户银行数据

cnBeta.COM5 月 3 日消息 外媒 BuzzFeed 报道，澳大利亚第一大商业银行澳大利亚联邦银行（CBA）证实，包含客户姓名，地址，账号和 2000 年至 2016 年的交易详情记录的两个存储磁带，在一次数据中心转运任务中被其分包商 Fuji-Xerox 丢失。其中至少包含 1200 万名用户的银行交易数据。当银行意识到这起事件时，其委托三方统计公司毕马威（KPMG）进行过一次独立的剖析调查，以了解具体情况，并通知了澳大利亚信息专员办公室（OAIC）。毕马威（KPMG）在调查后发现存储带很有可能已被处置，很难寻回。联邦银行的 Angus Sullivan 表示这些丢失的记录中没有包含任何可能危及客户账户安全的信息，比如密码或 PIN，目前仍无如何证据显示涉及的用户数据已经被利用或有任何可疑状况发生。

5、墨西哥央行证实金融机构支付系统遭黑客攻击 已展开调查

腾讯网 5 月 1 日消息 据外媒报道，墨西哥央行周一表示，当地至少有三家金融机构的支付系统遭到黑客攻击，但是没有资金被窃取。墨西哥央行正在调查这起攻击事件。墨西哥央行的支付系统负责人罗伦扎-马丁内兹（Lorenza Martinez）表示，两家银行和一家经纪公司与央行支付系统之间的网络连接受到了攻击。她否认了央行自身的支付系统已经被攻破的报道。墨西哥银行 Banorte 上周五表示，出现了一起事故，影响了该行与央行支付系统的连接。周一，Banorte 银行在回复路透社咨询的书面回应函中表示，它不是网络攻击的目标。不过，该公司没有提供任何细节，只是说“由于上周五的问题”，一些客户发现执行交易时出现了延迟。

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：何能强

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158