国家互联网应急中心

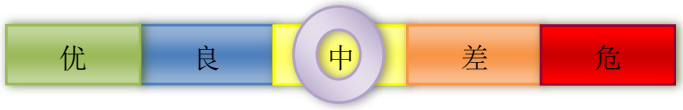
网络安全信息与动态周报

2020 年第 11 期

3 月 9 日-3 月 15 日

CNCERT/CC

本周网络安全基本态势

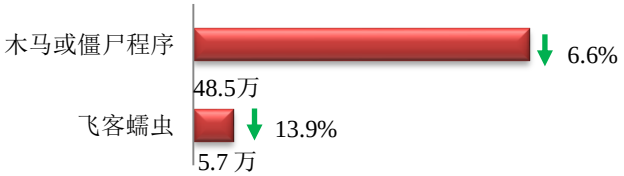


境内感染网络病毒的主机数量	•54.2万	↓ 7.4%
境内被篡改网站总数 其中政府网站数量	•8042 •28	↑ 6.8% ↑ 3.7%
境内被植入后门网站总数 其中政府网站数量	•1470 •1	↓ 6.8% ↓ 66.7%
针对境内网站的仿冒页面数量	•962	↓ 38.7%
新增信息安全漏洞数量 其中高危漏洞数量	•417 •138	↓ 24.7% ↓ 29.9%

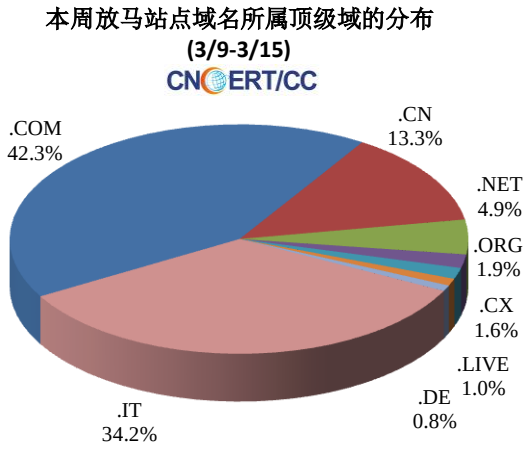
= 表示数量与上周相同　↑ 表示数量较上周环比增加　↓ 表示数量较上周环比减少

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 54.2 万个，其中包括境内被木马或被僵尸程序控制的主机约 48.5 万以及境内感染飞客（conficker）蠕虫的主机约 5.7 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 1205 个，涉及 IP 地址 4057 个。在 1205 个域名中，顶级域为.com 的约占 42.3%；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 316 个 IP。



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。

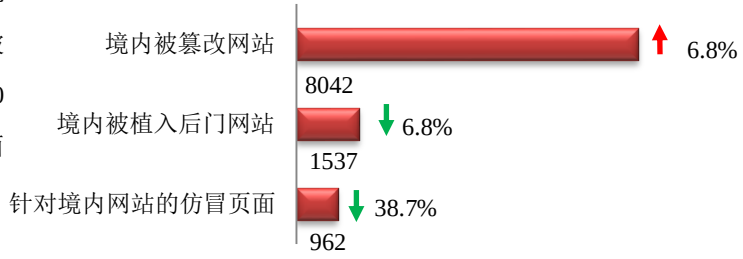
ANVA恶意地址黑名单发布地址

http://www.anva.org.cn/virusAddress/listBlack

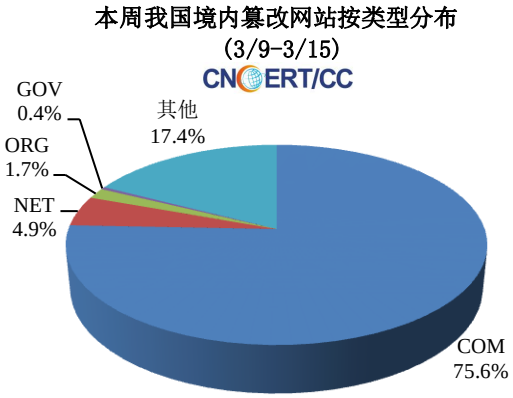
中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由中国互联网协会网络与信息安全工作委员会发起、CNCERT 具体组织运作的行业联盟。

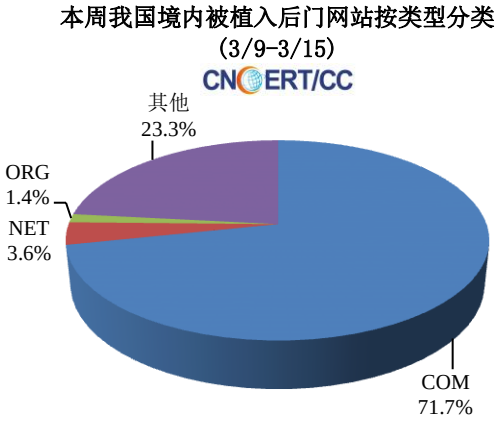
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 8042 个；被植入后门的网站数量为 1470 个；针对境内网站的仿冒页面数量 962 个。



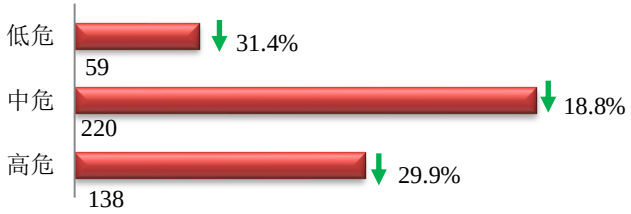
本周境内被篡改政府网站（GOV 类）数量为 28 个（约占境内 0.3%），较上周上涨了 3.7%；境内被植入后门的政府网站（GOV 类）数量为 1 个（约占境内 0.1%），较上周下降了 66.7%。

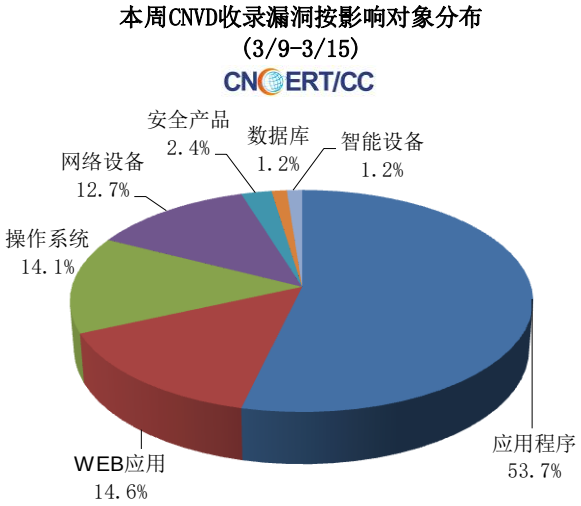




本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 417 个，信息安全漏洞威胁整体评价级别为中。





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 应用和操作系统。

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

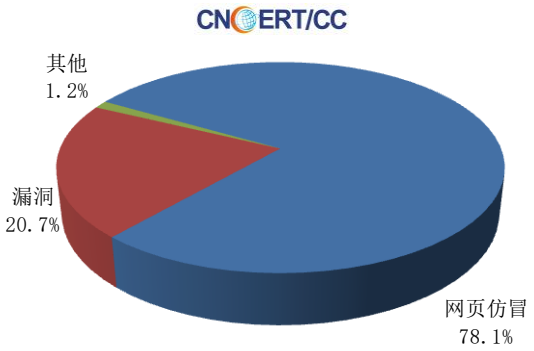
http://www.cnvd.org.cn/webinfo/list?type=4

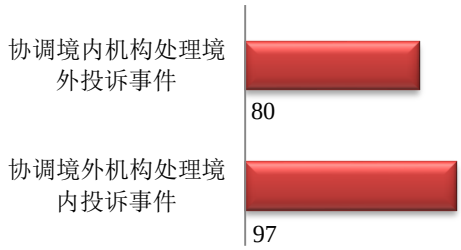
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 421 起，其中跨境网络安全事件 177 起。

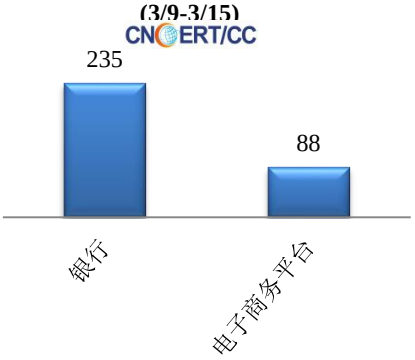
本周CNCERT处理的事件数量按类型分布
(3/9-3/15)



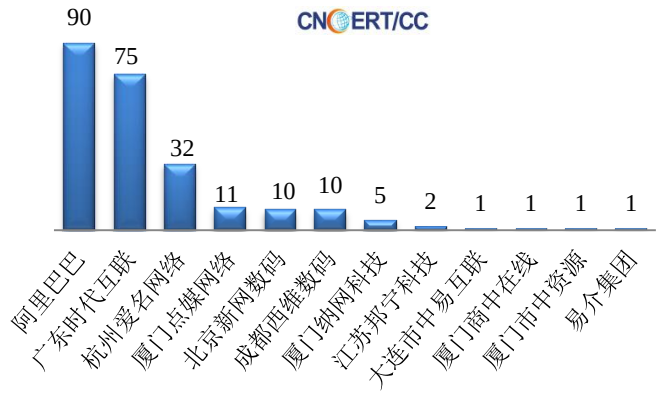


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 329 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包括银行仿冒事件 235 起和电子商务平台 88 起。

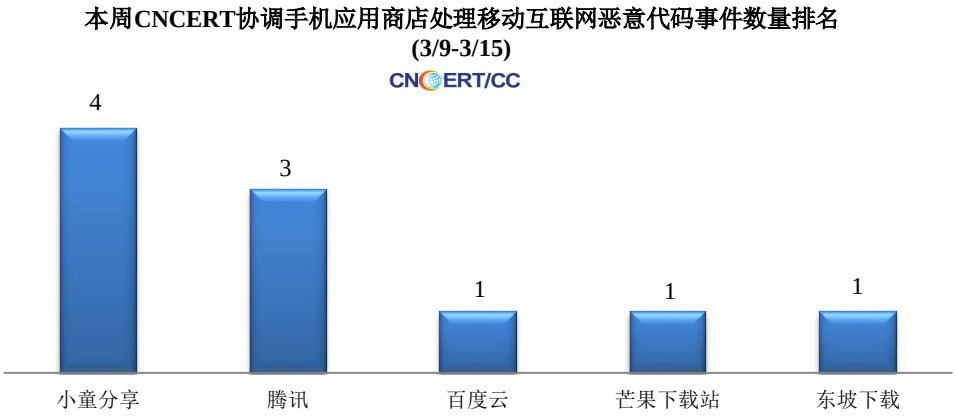
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计
(3/9-3/15)



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 (3/9-3/15)



本周，CNCERT 协调 5 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 10 个。



业界新闻速递

1、 全国信息安全标准化技术委员会发布《网络安全标准实践指南—远程办公安全防护》

3 月 13 日，全国信息安全标准化技术委员会发布了《网络安全标准实践指南—远程办公安全防护》（以下简称《实践指南》）的通知。《实践指南》给出了远程办公的典型应用场景，分析了远程办公可能面临的办公系统自身安全、数据安全、设备安全和个人信息保护等风险，针对远程办公系统的使用方和用户，分别给出了安全控制措施建议。其中，使用方应在管理和技术两方面开展安全防护，健全远程办公管理制度，加强运维管理，强化安全措施。用户应提高自身安全意识，重点针对设备、数据、环境等方面的安全风险进行防护。

2、 意大利黑客利用冠状病毒恐慌袭击当地用户

3 月 11 日，“E 安全”网站消息，IT 安全与保护公司 Sophos 相关专家发现一项新的勒索软件 TrickBot 正在利用意大利对冠状病毒（COVID-19）的关注度来针对意大利用户发起攻击。黑客将邮件伪装成是来自世界卫生组织工作人员的邮件，主题为“冠状病毒的重要信息”，其中的文件实际上是武器化的 Word 文档。该勒索软件不仅使攻击者从受感染的系统中收集信息，还试图进行横向移动以感染同一网络上的其他计算机，通过部署 Ryuk 病毒软件来获利。Sophos 的报告称，针对意大利的钓鱼攻击邮件正在加剧意大利人对本国冠状病毒爆发的担忧和恐惧。

3、 微软破获了全球最大僵尸网络 Necurs

3 月 11 日，外媒 The Register 消息，近日，微软联合 35 个国家的合作伙伴，共同破获了全球最大的网络犯罪僵尸网络 Necurs。微软表示，在最近 58 天的调查中，其工程师跟踪记录了 Necurs 网络中 1 台计算机，发现仅仅这 1 台电脑就在 2 个月的时间内发送了 380 万封电子邮件。此外，Necurs 网络也经常被出租给其他犯罪团伙，用来传播各种勒索软件、远程访问木马或盗取信息木马。据悉，Necurs 是迄今为止已知的全球最大垃圾邮件和恶意软件僵尸网络之一，已感染全球超过 900 万台计算机。微软最早在 2012 年就发现了该网络的存在，并将所有感染相同恶意软件模块的计算机命名为 Necurs，该模块会自动运行在用户的计算机上，并使用其资源每天发送大量垃圾邮件。微软已经获得法院授权，接管了 Necurs 在美国的现有域，并且预测了未来 25 个月内该网络可能创建的 600 万个域，通报给世界各地的域名管理机构，防止将来遭到攻击。

4、 Windows 严重蠕虫漏洞涉及 Win 10 多个版本

3 月 15 日，“E 安全”网站消息，3 月 10 日微软披露了一个 SMB 服务的重大安全漏洞，攻击者利用该漏洞无须权限即可实现远程代码执行。该漏洞有可能释放出一种自我复制攻击，从而使 WannaCry 和 NotPetya 破坏和削弱全球的商业网络。据悉，这一漏洞被标记为 CVE-2020-0796，该漏洞存在于 SMB 3.1.1 版本中，漏洞影响到 Windows 10 1903 之后的各个 32 位、64 位版 Windows，包括家用版、专业版、企业版、教育版。这些正是目前主流操作系统版本，在个人、企业环境中应用广泛。微软表示，成功利用这一漏洞的攻击者可以在使用这一漏洞协议的服务器和终端用户电脑上执行自己选择的代码。目前，微软已经投入了大量资源来加强对这类攻击的防御，并且已发布该漏洞的更新程序，以修补 Server Message Block 3.0（SMBv3）中的一个关键远程代码执行漏洞。与此同时，微软表示，可以通过禁用压缩功能进行系统保护，以阻止未经身份验证的攻击者利用此漏洞对 SMBv3 服务器的攻击。

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 与 76 个国家和地区的 233 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