国家互联网应急中心

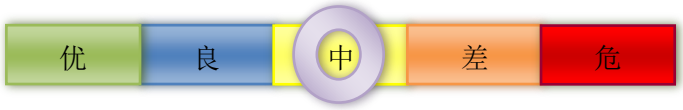
网络安全信息与动态周报

2020 年第 14 期

3 月 30 日-4 月 5 日

CNCERT/CC

本周网络安全基本态势

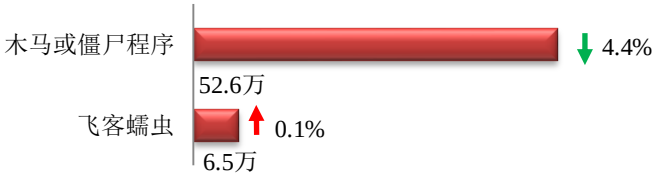


境内感染网络病毒的主机数量	•59.1万	↓ 3.9%
境内被篡改网站总数 其中政府网站数量	•8287 •37	↑ 9.7% ↑ 68.2%
境内被植入后门网站总数 其中政府网站数量	•1497 •5	↓ 8.9% ↓ 44.4%
针对境内网站的仿冒页面数量	•236	↓ 72.3%
新增信息安全漏洞数量 其中高危漏洞数量	•431 •207	↓ 14.5% ↓ 3.7%

= 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

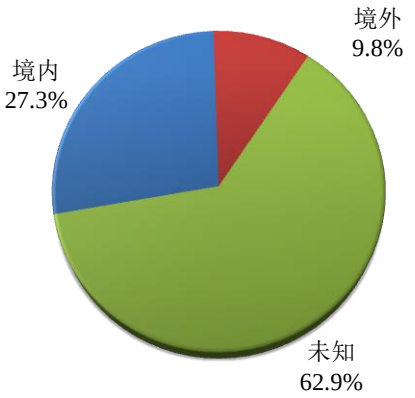
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 59.1 万个，其中包括境内被木马或被僵尸程序控制的主机约 52.6 万以及境内感染飞客（conficker）蠕虫的主机约 6.5 万。

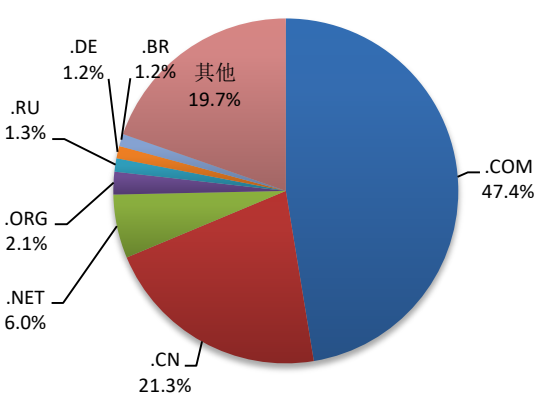


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 1038 个，涉及 IP 地址 4961 个。在 1038 个域名中，有 9.8%为境外注册，且顶级域为.com 的约占 47.4%；在 4961 个 IP 中，有约 49.5%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 419 个 IP。

本周放马站点域名注册所属境内外分布 (3/30-4/5)



本周放马站点域名所属顶级域的分布 (3/30-4/5)



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。

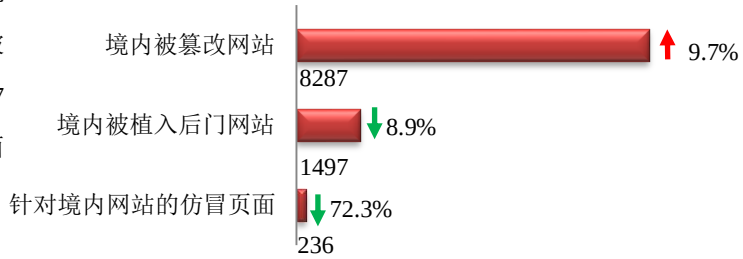
ANVA恶意地址黑名单发布地址

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。

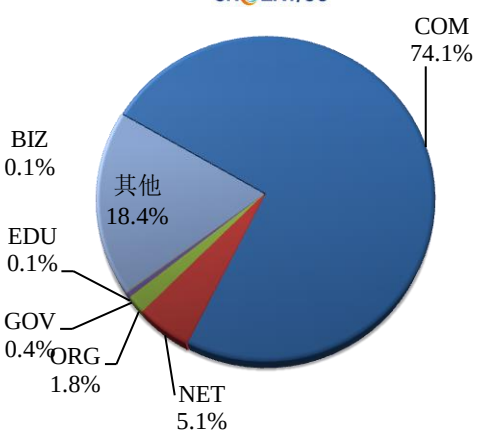
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 8287 个；被植入后门的网站数量为 1497 个；针对境内网站的仿冒页面数量 236 个。

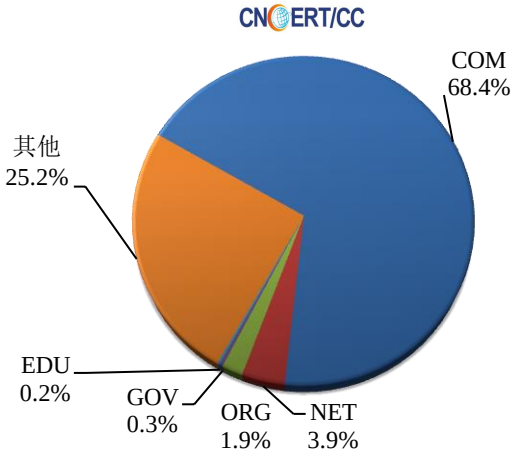


本周境内被篡改政府网站（GOV 类）数量为 37 个（约占境内 0.4%），较上周上涨了 68.2%；境内被植入后门的政府网站（GOV 类）数量为 5 个（约占境内 0.3%），较上周下降了 44.4%。

本周我国境内篡改网站按类型分布
(3/30-4/5)

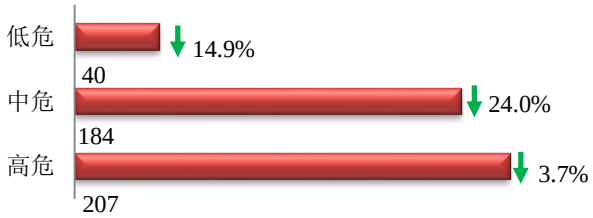


本周我国境内被植入后门网站按类型分类
(3/30-4/5)

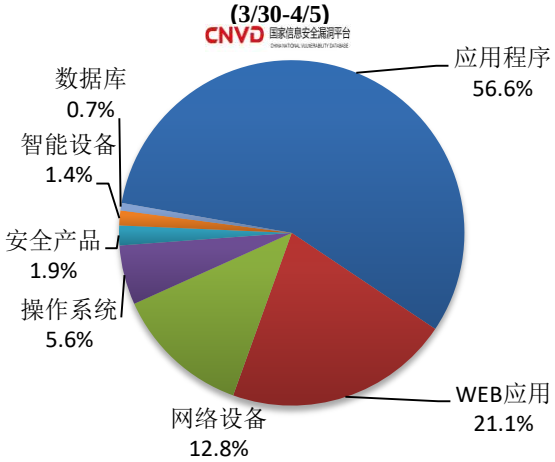


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 431 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
(3/30-4/5)



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。

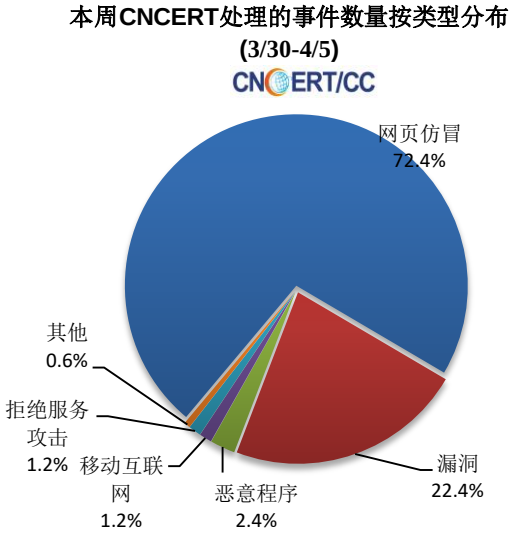
CNVD漏洞周报发布地址

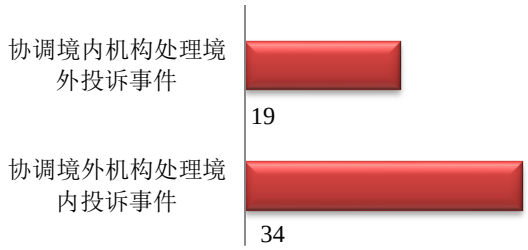
http://www.cnvd.org.cn/webinfo/list?type=4

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。

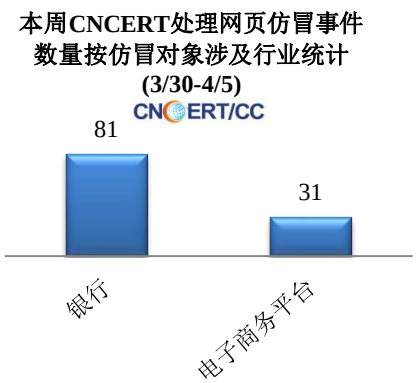
本周事件处理情况

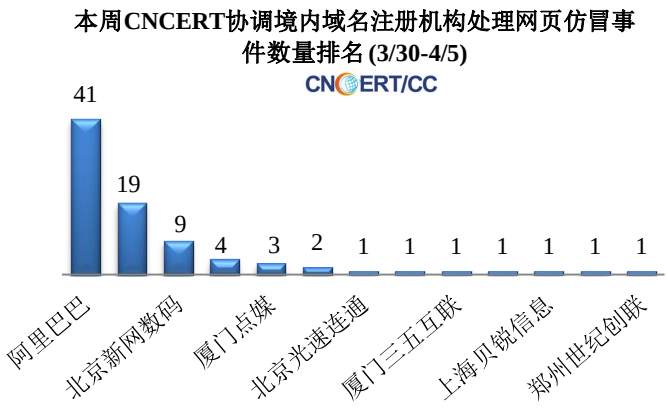
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 170 起，其中跨境网络安全事件 53 起。





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 123 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 81 起和电子商务平台 31 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 26 个。

业界新闻速递

1、 俄罗斯要求电子产品预装俄制软件的新立法被推迟生效

3 月 31 日，“CNBeat”网站消息，据外媒报道，俄罗斯要求所有智能手机、电脑和智能电视预装俄制软件的新立法被推迟，相关规定直到 2021 年 1 月才能生效。之前，俄罗斯议会下院于 2019 年 11 月通过立法，规定苹果 iPhone 等有预装应用程序的设备，必须预装俄罗斯制造的应用程序。这项立法针对的产品包括智能手机、电脑、平板电脑和智能电视。

2、 4200 万伊朗用户个人详细信息泄露 隐私安全遭严重威胁

4 月 1 日，“E 安全”消息，据外媒报道，研究人员发现托管在 Elasticsearch 服务器上的数据库配置发生错误，分析发现该数据库中包含了 4200 万伊朗公民个人的详细信息，包括用户帐户 ID、用户名、散列表、密钥和电话号码，而且该数据库被一群伊朗黑客上传在黑客论坛上进行售卖。在研究人员深入研究后，发现该数据来自由伊朗使用的 HotGram 和 Talagram 系统中，这二者是 Telegram 在伊朗的替代品。

3、 数以万计的私人 Zoom 录像被无意上传到视频云 任何人可在线观看

4 月 3 日，新闻网站 Mashable 报道，安全研究员爆料，近日成千上万的私人 Zoom 录像被视频会议发起者上传到了不同的视频网站和视频云，任何人都可以在网上观看。该研究员指出，这可能是有人将私人影像上传到公共服务器上的错误。不过，他们也指

出，如果 15000 人犯了错，那么可能是设计上的失误，而不是用户的粗心大意。Zoom 的发言人随后向 Mashable 发了一份声明，明确表示用户在将录音上传到网上时应谨慎行事。

4、 黑客清除 1.5 万多个 Elasticsearch 服务器

4 月 3 日，“ZDNet”网站消息，在过去的两周里，黑客一直入侵没有密码保护的在互联网上保持打开状态的 Elasticsearch 服务器，试图擦除数据库中的内容，并留下了某网络安全公司的名称，以试图转移责任。安全研究人员约翰·威辛顿（John Wethington）称，经分析发现第一次入侵应该始于 3 月 24 日左右。该黑客应该是制作了自动扫描脚本在互联网上广泛扫描不受保护的 ElasticSearch 系统，连接后尝试擦除内容，并创建一个新的空索引。

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：马莉雅

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315