国家互联网应急中心

网络安全信息与动态周报

2019 年第 4 期

1 月 21 日-1 月 27 日

CNCERT/CC

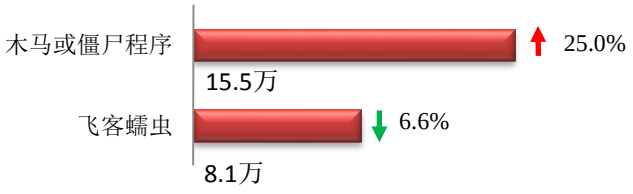
本周网络安全基本态势

境内感染网络病毒的主机数量	•23.6万	↑12.0%
境内被篡改网站总数 其中政府网站数量	•701 •42	↑9.9% ↓2.3%
境内被植入后门网站总数 其中政府网站数量	•600 •3	↑7.0% ↓66.7%
针对境内网站的仿冒页面数量	•1260	↓26.7%
新增信息安全漏洞数量 其中高危漏洞数量	•177 •65	↓52.8% ↓40.9%

=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

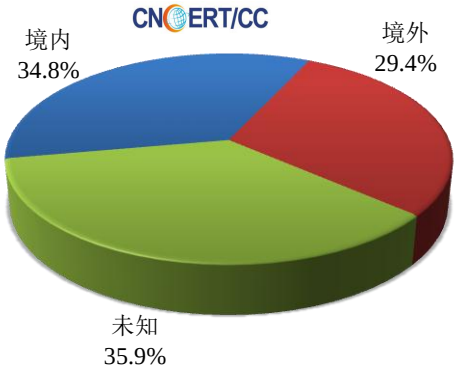
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 23.6 万个，其中包括境内被木马或被僵尸程序控制的主机约 15.5 万以及境内感染飞客（conficker）蠕虫的主机约 8.1 万。

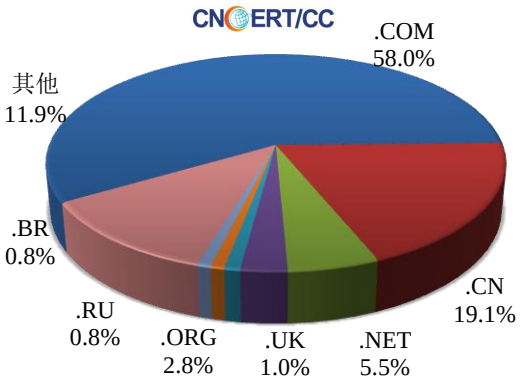


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 3245 个，涉及 IP 地址 5331 个。在 3245 个域名中，有 29.4%为境外注册，且顶级域为.com 的约占 58.0%；在 5331 个 IP 中，有约 56.0%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 587 个 IP。

本周放马站点域名注册所属境内外分布
(1/21-1/27)



本周放马站点域名所属顶级域的分布
(1/21-1/27)



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。

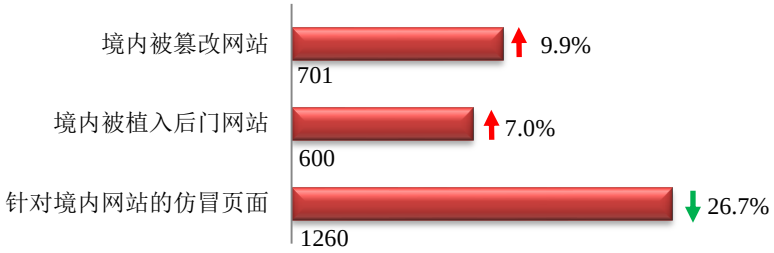
ANVA恶意地址黑名单发布地址

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。

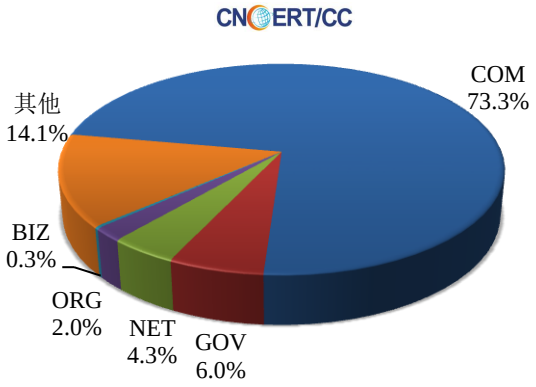
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 701 个；境内被植入后门的网站数量为 600 个；针对境内网站的仿冒页面数量\1260 个。

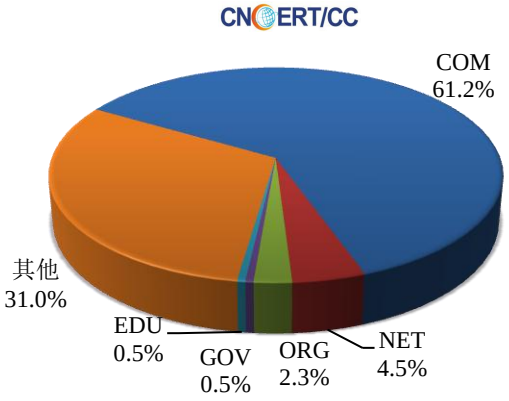


本周境内被篡改政府网站（GOV 类）数量为 42 个（约占境内 6.0%），较上周环比下降了 2.3%；境内被植入后门的政府网站（GOV 类）数量为 3 个（约占境内 0.5%），较上周环比下降了 66.7%；针对境内网站的仿冒页面涉及域名 77 个，IP 地址 194 个，平均每个 IP 地址承载了约 32 个仿冒页面。

本周我国境内被篡改网站按类型分布
(1/21-1/27)

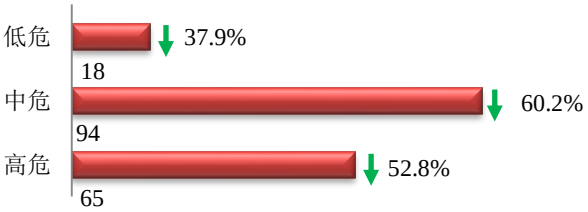


本周我国境内被植入后门网站按类型分布
(1/21-1/27)

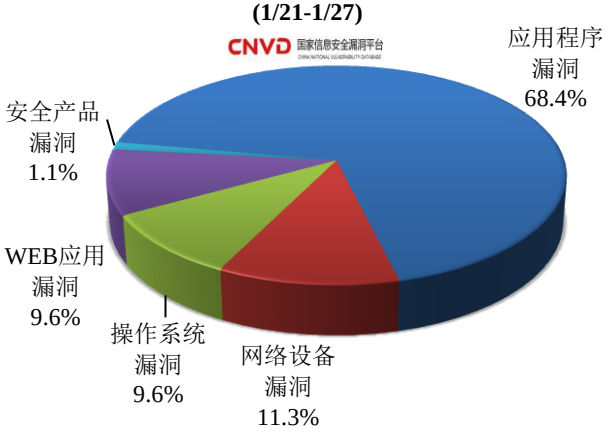


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 177 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
(1/21-1/27)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是网络设备漏洞。

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

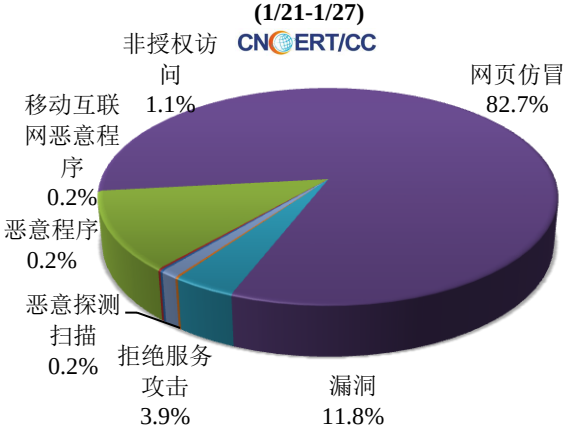
http://www.cnvd.org.cn/webinfo/list?type=4

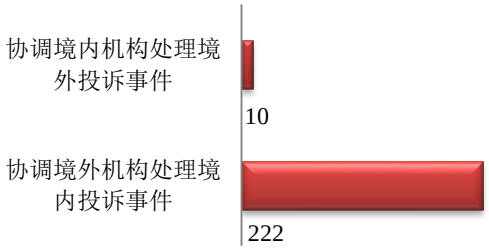
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 542 起，其中跨境网络安全事件 232 起。

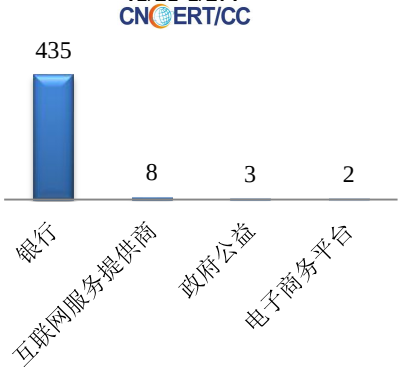
本周CNCERT处理的事件数量按类型分布 (1/21-1/27)



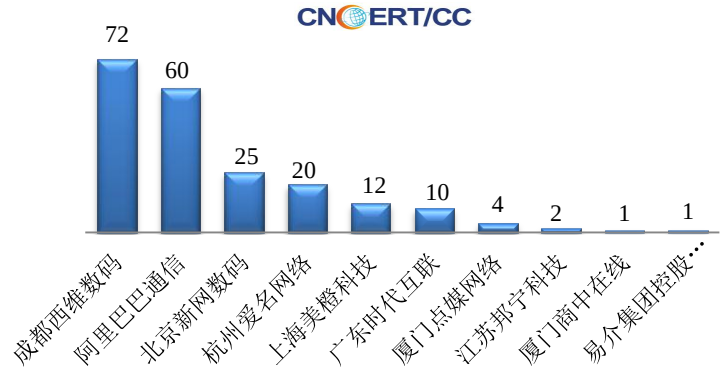


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 448 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 435 起和互联网服务提供商仿冒事件 8 起。

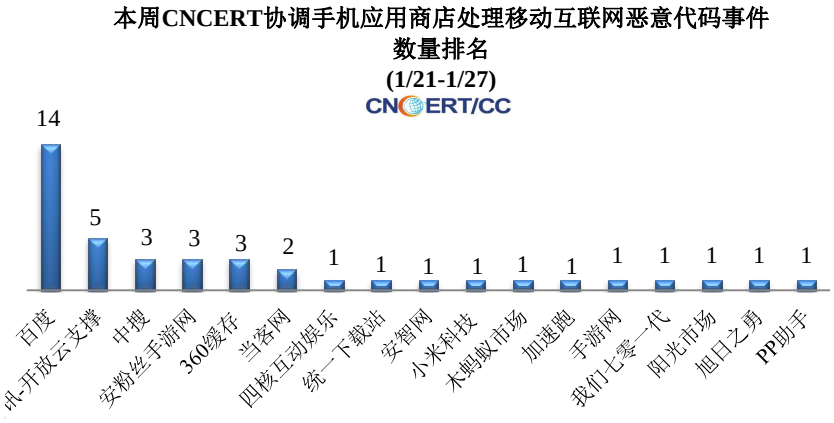
本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (1/21-1/27)



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 (1/21-1/27)



本周，CNCERT 协调 17 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 41 个。



业界新闻速递

1、四部委联合开展“App 违法违规收集使用个人信息专项治理”

人民网 1 月 26 日消息 中央网信办、工信部、公安部、市场监管总局等四部门召开新闻发布会，联合发布《关于开展 App 违法违规收集使用个人信息专项治理的公告》。为切实治理个人信息保护方面存在的乱象，四部门决定自 2019 年 1 月至 12 月，在全国范围组织开展 App 违法违规收集使用个人信息专项治理。《公告》指出，App 运营者收集使用个人信息时要严格履行《网络安全法》规定的责任义务，对获取的个人信息安全负责，采取有效措施加强个人信息保护。遵循合法、正当、必要的原则，不收集与所提供服务无关的个人信息；收集个人信息时要以通俗易懂、简单明了的方式展示个人信息收集使用规则，并经个人信息主体自主选择同意；不以默认、捆绑、停止安装使用等手段变相强迫用户授权，不得违反法律法规和与用户的约定收集使用个人信息。倡导 App 运营者在定向推送新闻、时政、广告时，为用户提供拒绝接收定向推送的选项。

2、欧洲国家聚焦网络安全和隐私保护问题

新华社 1 月 22 日消息 第 11 届国际网络安全论坛 22 日在法国北部城市里尔拉开帷幕，本届论坛的主题为“定制安全和隐私”。超过 8500 名欧洲网络安全官员、专家及从业者与会。论坛为期两天，将通过会展、研讨等形式推动欧洲网络安全发展。网络安全不仅仅指信息安全和信息系统安全，还包括国家、社会等广义层面的安全。

3、美国不受保护的政府服务器泄露了 FBI 多年的调查信息

E 安全 1 月 21 日消息 据外媒报道，美国俄克拉荷马州证券部门（简称 ODS）的存储服务器至少一个星期未得到保护，如今多达 3TB 的政府数据遭泄露，共含数百万敏感文件。网络安全公司 UpGuard 的研究员

GregPollock 发现这个存储服务器不安全的问题。该服务器中还有俄克拉荷马州证券委员会（Oklahoma Securities Commission）数十年的机密文件，以及美国联邦调查局（FBI）的调查文件。现在任何人都可以访问这些文件。除此之外，遭泄露的信息还包括了电子邮件、社会保险号、1 万名经纪人的姓名和地址、远程访问 ODS 工作站的凭证、准备提交给俄克拉荷马州证券委员会的通讯信息，以及与艾滋病患者相关的资料。

4、美国多家大银行泄露大量贷款文件：数量有 2400 多万份

cnBeta.COM1 月 24 日消息 因服务器出现安全漏洞，美国多家大银行泄露 2400 多万份金融及银行资料，涉及大量贷款和抵押贷款信息。受影响的服务器上运行 Elasticsearch 数据库，里面包含了 10 多年的历史数据，比如贷款和抵押贷款协议、还款计划、敏感财务及税务文档。这些文件没有受到密码的保护，任何人都可以查阅。泄露可以追溯到德克萨斯州金融数据及分析公司 Ascension，它提供数据分析、投资组合估值分析服务。在服务过程中，Ascension 将纸制文档、手写文本转化为计算机可以阅读的文件。Ascension 母公司 Rocktop Partners 的高管证实，服务器出现漏洞，不过系统没有受到影响。1 月 15 日，供应商在配置服务器时出现错误，导致一些与抵押贷款有关的文档泄露。不过供应商很快关闭了问题服务器，Rocktop Partners 正在与第三方专家合作展开调查。

5、谷歌违反通用数据保护条例遭法国当局罚款 5000 万欧元

新浪科技 1 月 22 日消息，谷歌已因违反“通用数据保护条例”（GDPR）而被法国数据保护监管机构处以 5000 万欧元（约合 5680 万美元）罚款，这对马克斯·施雷姆斯(Max Schrems)旗下隐私集团 NOYB 来说是一场胜利。法国国家互联网信息中心（以下简称“CNIL”）今日裁定，谷歌向用户提供了不充分的信息，在多个页面上分散提供信息，而且并未在广告个性化的问题上获得有效许可。CNIL 对 NOYB 和法国数字版权组织 La Quadrature du Net 提出的投诉作出了反应，称其已对通过 Android 设备开设谷歌账户的流程进行了调查。这个监管机构作出的结论是，谷歌在两个方面违反了“通用数据保护条例”：一是未满足透明度和信息相关要求，二是没有为其处理流程获得法律依据。根据这项条例，违规公司可被处以最高 2000 万欧元或相当于年度营业额 4%的罚款，而 CNIL 已经行使了这种新的权力，向谷歌开出了 5000 万欧元的罚单。

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：郭晶

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158