国家互联网应急中心

2019 年第 18 期
4 月 29 日-5 月 5 日

网络安全信息与动态周报

本周网络安全基本态势

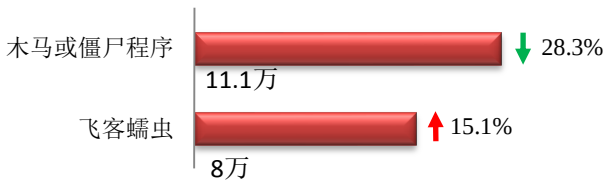
优 | 良 | 中 | 差 | 危

境内感染网络病毒的主机数量	• 19.0万	↓ 14.9%
境内被篡改网站总数[1] 其中政府网站数量	• 5573 • 17	↑ 51.4% ↓ 65.3%
境内被植入后门网站总数 其中政府网站数量	• 1001 • 16	↓ 42.1% ↑ 14.3%
针对境内网站的仿冒页面数量	• 1979	↑ 33.0%

= 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 19.0 万个，其中包括境内被木马或被僵尸程序控制的主机约 11.1 万以及境内感染飞客（conficker）蠕虫的主机约 8.0 万。



[1]本期境内被篡改网站数量受监测数据范围扩大影响，波动较大

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。

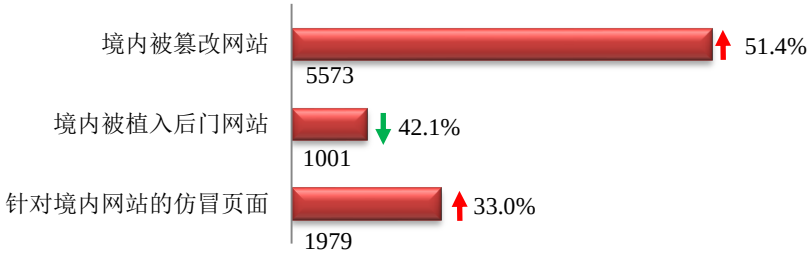
ANVA恶意地址黑名单发布地址

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。

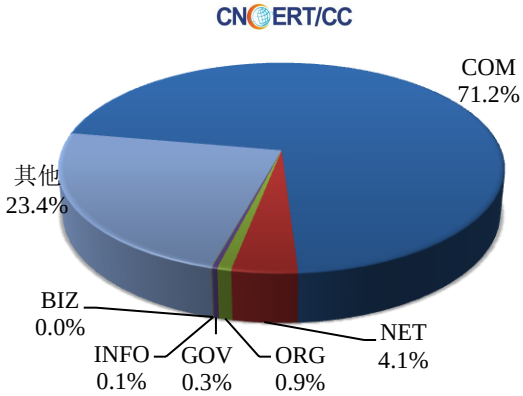
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 5573 个；境内被植入后门的网站数量为 1001 个；针对境内网站的仿冒页面数量 1979 个。

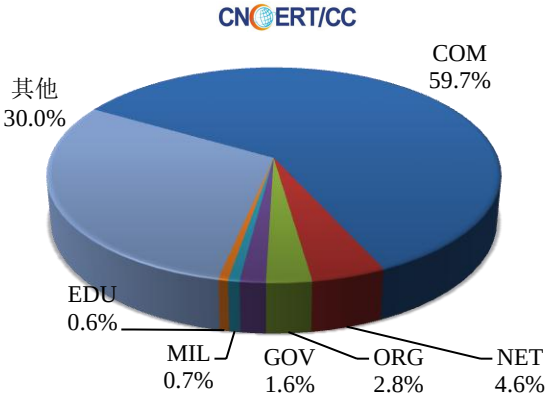


本周境内被篡改政府网站（GOV 类）数量为 17 个（约占境内 0.3%），较上周环比下降 65.3%；境内被植入后门的政府网站（GOV 类）数量为 16 个（约占境内 1.6%），较上周环比上升 14.3%；针对境内网站的仿冒页面涉及域名 505 个，IP 地址 312 个，平均每个 IP 地址承载了约 6 个仿冒页面。

本周我国境内被篡改网站按类型分布
(4/29-5/5)

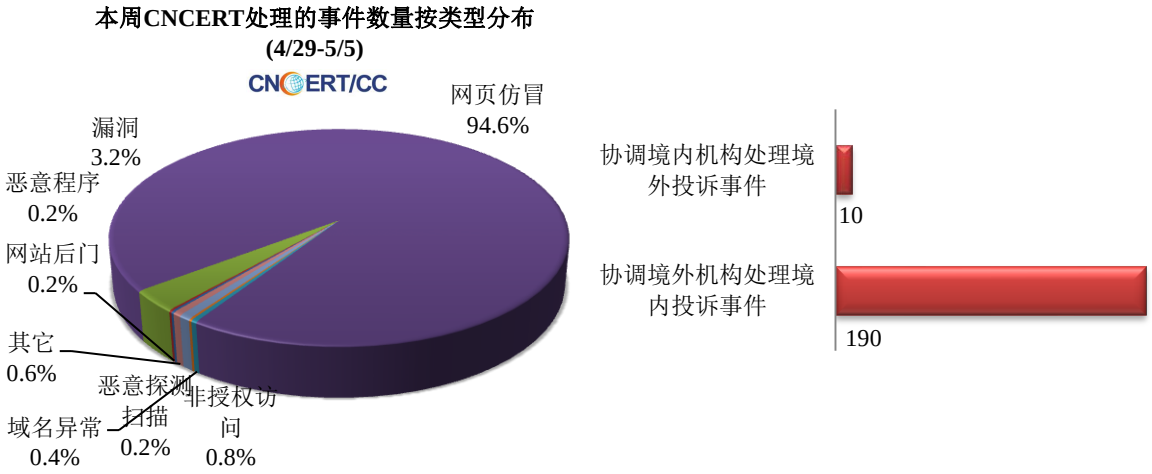


本周我国境内被植入后门网站按类型分布
(4/29-5/5)

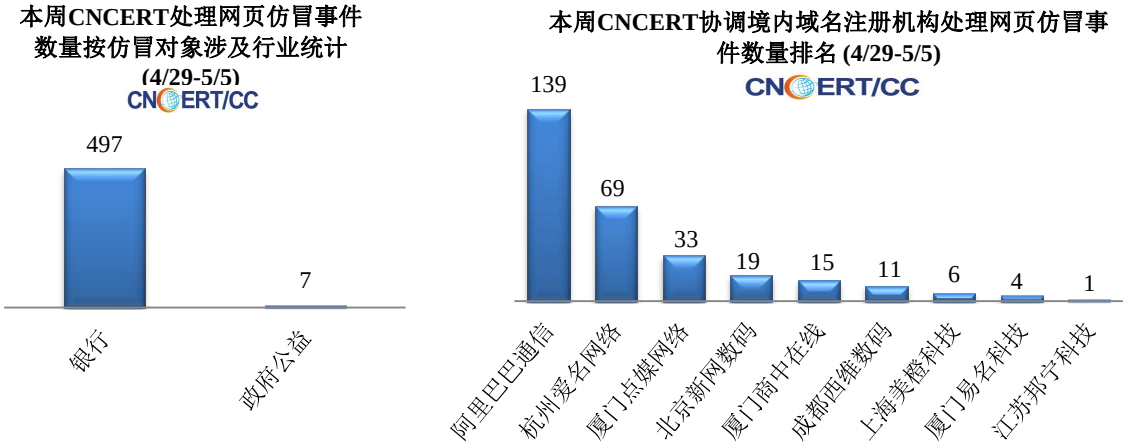


本周事件处理情况

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 533 起，其中跨境网络安全事件 200 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 504 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 497 起和政府公益事件 7 起。



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 13 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 (4/29-5/5)

业界新闻速递

1、俄总统签署防范外部“断网”风险的法律

新华社莫斯科 5 月 1 日消息 俄罗斯总统普京签署法律文件，以确保俄罗斯互联网在遭遇外部“断网”等冲击时仍能稳定运行。根据普京签署的法律，俄罗斯将建立本国的域名系统，即存储和获取网络地址及域名信息的系统。俄联邦电信、信息技术和大众传媒监督局将成立网络监控管理中心，负责在出现外部异常情况时保障俄境内网络通信服务运行，并协调各网络通信运营商应对。

2、印度将成立国防网络机构应对黑客威胁

安全内参 5 月 1 日消息 为了提高印度应对黑客威胁的能力，印度将于 5 月成立国防网络机构（Defence Cyber Agency ，简称 DCA），总部设在首都新德里。DCA 将与军队合作，共同应对网络威胁，并将包含 DRDO（国防研究与发展组织）的元素。该网络机构的部队将遍布全国。每个分支都将有专门的单位或小组来处理网络安全方面的问题。

3、黑客攻击 Docker Hub，19 万用户数据遭泄露

E 安全 4 月 30 日消息 Docker Hub 遭黑客攻击，虽然黑客只访问数据库的时间很短，但是依然有 19 万用户的数据遭泄露。Docker Hub 于 4 月 26 日宣布黑客利用了一个安全漏洞暴露了 Docker Hub 的用户名、哈希密码、GitHub 和 Bitbucket 访问令牌。Docker 已通知用户重置密码，并撤销了 GitHub 令牌和访问密钥，要求用户重新

连接到存储库，检查安全日志。公司还建议用户查看 GitHub 和 Bitbucket 账户登录日志，查看是否有来自未知 IP 地址的访问。

4、神秘数据库泄露 8000 万美国人的个人数据

E 安全 5 月 1 日消息 一个神秘数据库暴露了近 8000 万美国人的个人信息，影响了 65%的美国家庭。安全研究人员发现了在微软云服务器上托管的 24 GB 数据库。该数据库包含美国家庭的高度敏感信息，其中包括家庭成员的全名、婚姻状况、收入、年龄等。根据 VPNMentor 的报告，该数据库以家庭的形式列出信息，其中包括家庭住址、准确经纬度、家庭成员全名、年龄、出生日期。除此之外，还有性别、婚姻状况、收入、房主状况和居住类型的编码。此次泄露的个人数据可能导致受害者容易遭受垃圾邮件、网络钓鱼、勒索软件等网络攻击。

5、几大 Git 平台仓库被劫 黑客欲勒索比特币

cnBeta.COM5 月 4 日消息 数百名开发人员的 Git 仓库被黑客删除，取而代之的是赎金要求。攻击于 5 月 3 日开始，包括 GitHub、Bitbucket 和 GitLab 在内的代码托管平台都受到了影响。目前已知的情况是，黑客从受害者的 Git 仓库中删除了所有源代码和最近提交的 Repo，只留下了 0.1 比特币（约 ¥3850）的赎金票据。黑客声称所有源码都已经下载并存储在他们的一台服务器上，并且给受害者十天时间支付赎金，否则，他们会公开代码。

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：肖崇蕙

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158