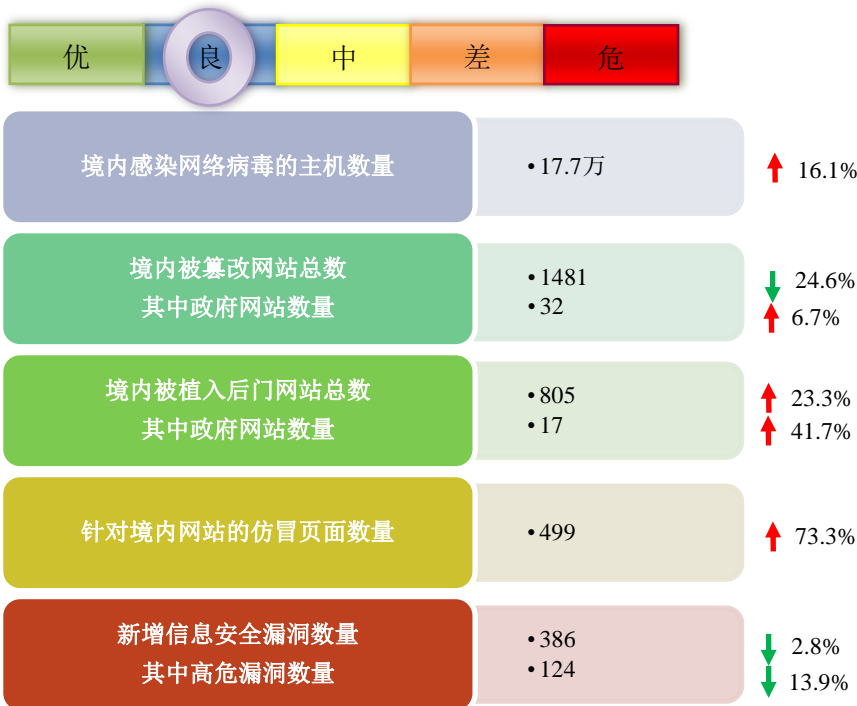


网络安全信息与动态周报

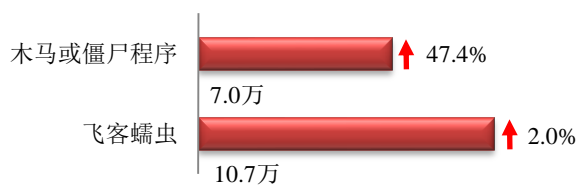
本周网络安全基本态势



■ 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

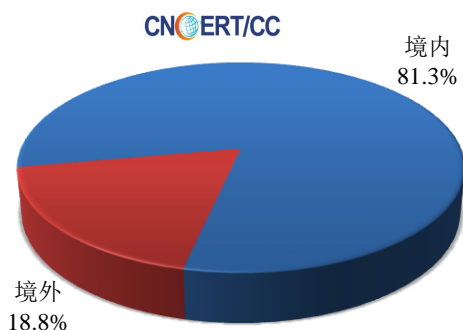
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 17.7 万个，其中包括境内被木马或被僵尸程序控制的主机约 7.0 万以及境内感染飞客（conficker）蠕虫的主机约 10.7 万。

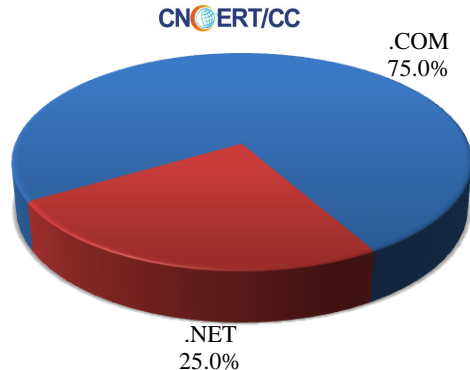


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 16 个，涉及 IP 地址 41 个。在 16 个域名中，有 18.8% 为境外注册，且顶级域为 .com 的约占 75.0%；在 41 个 IP 中，有约 26.8% 位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 0 个 IP。

本周放马站点域名注册所属境内外分布
(3/5-3/11)



本周放马站点域名所属顶级域的分布
(3/5-3/11)



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。

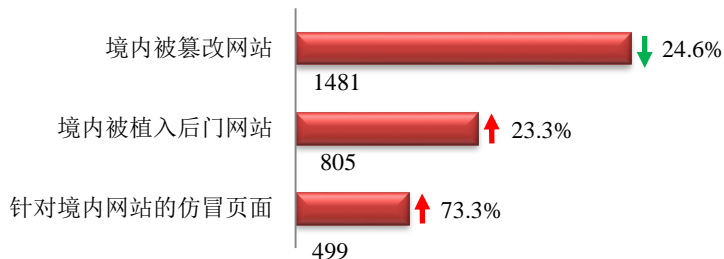
ANVA 恶意地址黑名单发布地址

<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。

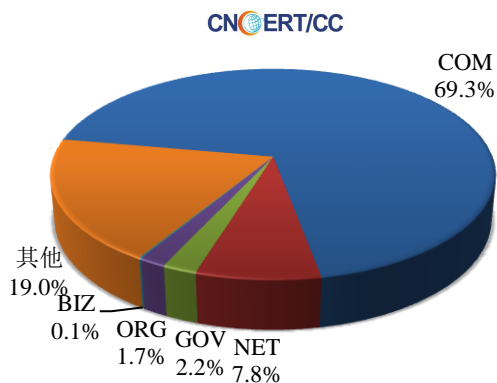
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1481 个；境内被植入后门的网站数量为 805 个；针对境内网站的仿冒页面数量为 499。

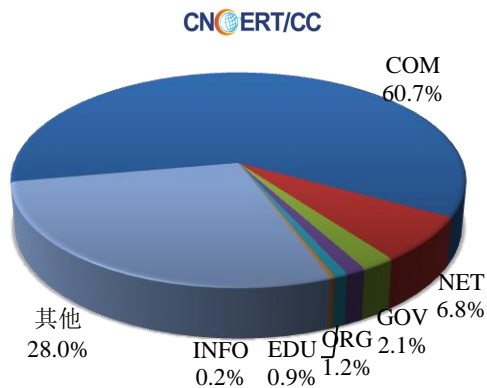


本周境内被篡改政府网站（GOV 类）数量为 32 个（约占境内 2.2%），较上周环比上升了 6.7%；境内被植入后门的政府网站（GOV 类）数量为 17 个（约占境内 2.1%），较上周环比上升了 41.7%；针对境内网站的仿冒页面涉及域名 424 个，IP 地址 147 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内被篡改网站按类型分布
(3/5-3/11)

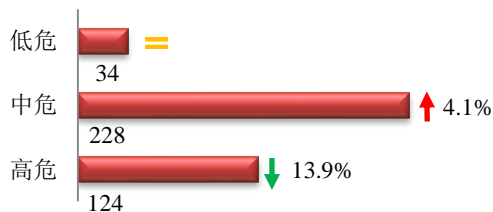


本周我国境内被植入后门网站按类型分布
(3/5-3/11)

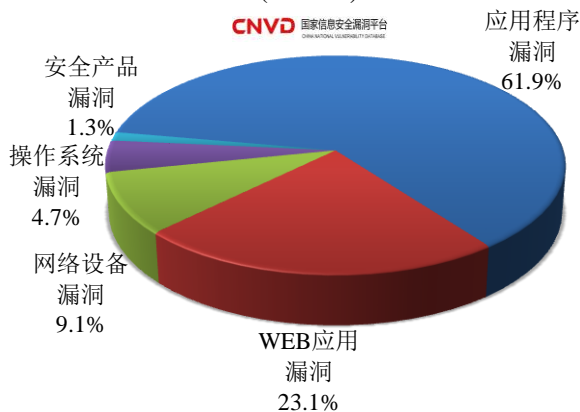


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 386 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
(3/5-3/11)



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

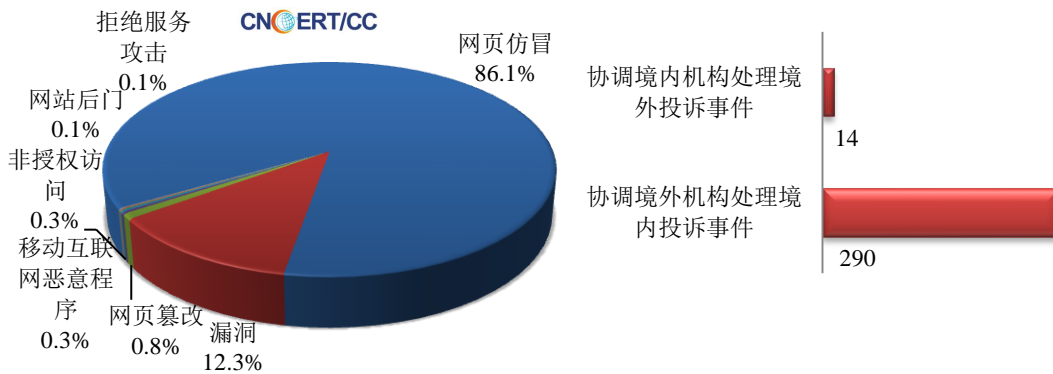
<http://www.cnvd.org.cn/webinfo/list?type=4>

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

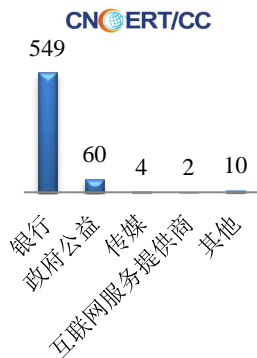
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 726 起，其中跨境网络安全事件 304 起。

本周CNCERT处理的事件数量按类型分布
(3/5-3/11)

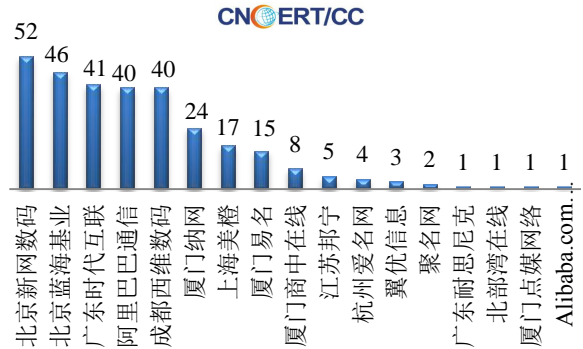


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 625 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 549 起和政府公益仿冒事件 60 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(3/5-3/11)

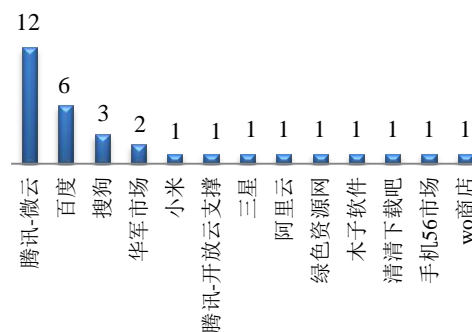


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名(3/5-3/11)



本周，CNCERT 协调 13 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 32 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
(3/5-3/11)
CNCERT/CC



业界新闻速递

1、欧盟将建立网络安全与防御培训教育平台

搜狐网 3 月 7 日消息 据欧洲防务局 2018 年 2 月 28 日报道,日前, 欧盟一致通过构建一个共用服务平台的决议, 用于在网络安全和防御领域为各成员国提供教育、训练、演习和评估 (ETEE)。欧洲安全与防务学院 (European Security and Defence College, ESDC) 将负责该平台的建设和运行, 而欧洲防务局 (European Defence Agency, EDA)、欧洲对外行动署 (European External Action Service, EEAS) 和欧盟委员会 (European Commission) 已经对该平台的建设提供相应资助。教育、训练、演习和评估共用平台的主要功用是为欧盟各成员国提供网络安全和防御培训和教育。为此, 现有的培训将被调整和统一化, 而新平台将会弥补培训需求和培训活动之间的差距。该工作将由各利益相关方和合作伙伴共同推进。在欧盟-北约联合声明框架内, 欧洲安全与防务学院也将参照北约颁布的各种举措, 发挥其与该平台的协同效应。该网络平台预期 2018 年 9 月 1 日达到初始运行能力。2019 年 4 月, 具备完善功能的网络安全和防务平台将正式上线运行。

2、日本拟修改通信相关法 为打击网络攻击共享信息

中新网 3 月 6 日消息 据日媒报道, 日本政府 3 月 6 日在内阁会议上敲定了《电气通信事业法》和《情报通信研究机构 (NICT) 法》修正案, 写入了为加强打击网络攻击的措施, 通信商之间推进信息共享的新制度。日本政府力争让修正案在本届国会获得通过。据报道, 修正案中新设了由通信商将长期不用的电话号码交还政府的制度, 以应对电话号码需求的增加。此外修正案还提出要出台通信商在关停对用户影响较大的通信服务时有义务事先申报的制度。报道指出, 在日本, 随着监控探头和各种传感器等物联网 (IoT) 设备的普及, 劫持设备引起网上故障的网络攻击与日俱增。日本政府欲通过修改法律使各通信商通过第三方机构共享有关网络攻击的信息, 从而能迅速阻断攻击。另一方面, 由于密码设定简单的物联网设备容易成为劫持的对象, 拟允许 NICT 对设备密码设定是否存在疏漏展开调查。若存在疏漏, 将通过通信商提醒设备使用者引起重视, 敦促其整改。

3、2700 万能源智能电表存在安全漏洞，英国情报机构 GCHQ 发布物联网安全预警

HackerNews.cc 3 月 6 日消息 外媒 3 月 4 日消息，英国情报机构政府通信总部 GCHQ 发现安装在 2700 万个家庭中的新型智能电表存在安全漏洞，可能会对数百万布列塔尼人（西欧法国西北部布列塔尼半岛上的居民）的物联网设备构成严重风险。据“每日电讯报”报道，GCHQ 认为智能电表存在安全隐患：攻击者能够窃取智能电表用户的个人信息，并且通过篡改账单来获取利益。除此之外，文章也透露了其他方面上智能电表可能会引起的问题。GCHQ 警告称攻击者能够使用这些存在漏洞的设备作为“特洛伊木马”进入客户的网络。英国政府担心某些国家的黑客开勇能源智能电表的缺陷造成电力飙升，从而损害国家电网。安全专家也表示，BlueBorne 攻击可能会通过利用蓝牙连接来将智能电表暴露给黑客。

4、印度国有电信运营商内部网站存漏洞，超 4.7 万员工信息泄露

E 安全 3 月 6 日消息 根据《印度经济时报（The Economic Times,ET）》及多家国外媒体的报道，法国安全研究人 Robert Baptiste 声称已获得印度国有电信运营商 Bharat Sanchar Nigam Limited（BSNL）内部网络数据库的访问权，该数据库包含超过 4.7 万名员工的详细信息。Baptiste 通过电子邮件与 ET 取得了联系并告诉 ET，他通过安全漏洞侵入了 BSNL 的内部网络，并将恶意代码嵌入在了 BSNL 所使用的软件中，以此获取到了数据库的访问权限。在上周日早上，Baptiste 还与 ET 分享了一个包含 BSNL 离职和现任员工姓名、职称、密码、手机号码、出生日期、退休日期、电子邮件地址等详细信息的数据库样本。ET 随后从数据库中调取了六名员工的个人信息，并通过电话验证了他们的身份属实。Baptiste 还表示，BSNL 所持域名下的多个网站均存在安全漏洞，使得这些网站极易遭受 SQL 注入攻击。事实上，已经有两个 BSNL 网站遭遇了勒索软件的攻击，但网站受到攻击的确切时间尚不清楚，目前网站已经被迫下线。而 Baptiste 还发现，多达八个其他 BSNL 网站具有开放的目录，允许任何人访问数据库。

5、日本知名游戏开发商 NIS 美国分部在线商城的客户支付卡数据被盗

HackerNews.cc 3 月 7 日消息 外媒 3 月 5 日消息，日本游戏开发商 Nippon Ichi Software 透露，其美国分公司 NIS America 的网上商城 store.nisamerica.com 和 snkonlinestore.com 于 1 月 23 日至 2 月 26 日的某个时间段遭受了严重的数据泄露，可能会影响在线客户的个人信息和财务数据。根据 NIS America 上周向受影响客户发的一封电子邮件得知，该公司在 2 月 26 日上午发现其结账页面被链接了一个恶意程序，具体流程为：黑客设法在用户下单后获取其付款卡细节和个人信息，然后恶意程序将用户返回到 NIS America 存储页面，以完成进一步的欺骗交易。邮件中并未提及具体有多少客户在此次事件中受到了影响，也没有提供进一步的攻击详情。为了表示歉意，该公司通过其在线商店向客户提供了 5 美元的优惠折扣。

6、AWS 存储桶泄露 50.4 GB 数据，金融巨头受影响

E 安全 3 月 11 日消息 云安全厂商 UpGuard 公司网络风险小组发现一批由于 Amazon Web Services（简称 AWS）S3 存储桶未受保护而泄露的 50.4 GB 数据。经证实，此 AWS 存储桶属于云商务智能（简称 BI）与分析厂商 Birst 公司。这 50.4GB 数据涉及 Birst 公司主要客户 Capital One（一家位于弗吉尼亚州麦克莱恩市的金融服务巨头，亦为全美第八大商业银行），包含 Capital One 网络基础设施配置信息以及 Birst 公司的设备技术信息。

根据 UpGuard 公司发布的官方微博文，这批数据当中包含密码、管理访问凭证以及私钥，且专供 Birst 公司内部云环境中的 Capital One 相关系统使用。攻击者利用这批遭到泄露的数据足以掌握 Capital One 对 Birst 设备的使用方式，进而入侵 IT 系统并深入挖掘该公司的内部资讯。

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：朱芸茜

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158