国家互联网应急中心

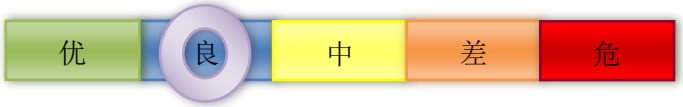
网络安全信息与动态周报

2018 年第 11 期

3 月 12 日-3 月 18 日

CNCERT/CC

本周网络安全基本态势

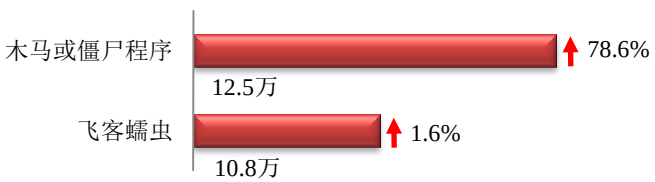


境内感染网络病毒的主机数量	•23.3万	↑ 32.1%
境内被篡改网站总数 其中政府网站数量	•937 •33	↓ 36.7% ↑ 3.1%
境内被植入后门网站总数 其中政府网站数量	•1028 •32	↑ 27.7% ↑ 88.2%
针对境内网站的仿冒页面数量	•751	↑ 50.5%
新增信息安全漏洞数量 其中高危漏洞数量	•460 •130	↑ 19.2% ↑ 4.8%

═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

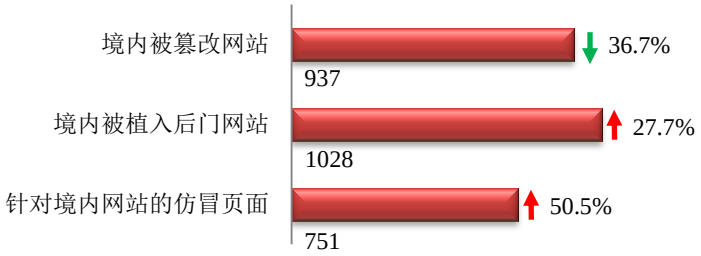
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 23.3 万个，其中包括境内被木马或被僵尸程序控制的主机约 12.5 万以及境内感染飞客（conficker）蠕虫的主机约 10.8 万。



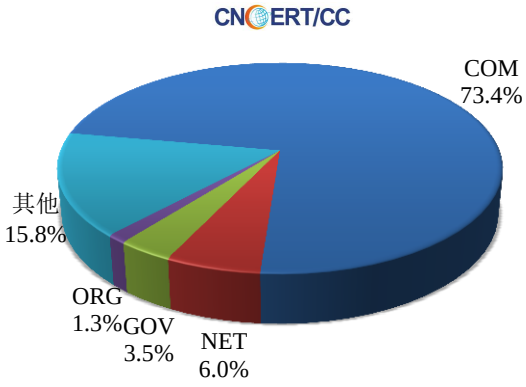
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 937 个；境内被植入后门的网站数量为 1028 个；针对境内网站的仿冒页面数量为 751。

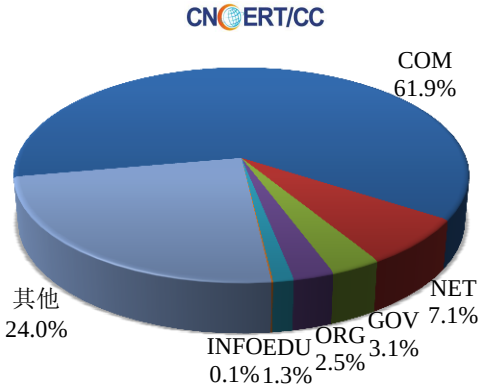


本周境内被篡改政府网站（GOV 类）数量为 33 个（约占境内 3.5%），较上周环比上升了 3.1%；境内被植入后门的政府网站（GOV 类）数量为 32 个（约占境内 3.1%），较上周环比上升了 88.2%；针对境内网站的仿冒页面涉及域名 322 个，IP 地址 142 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被篡改网站按类型分布
(3/12-3/18)

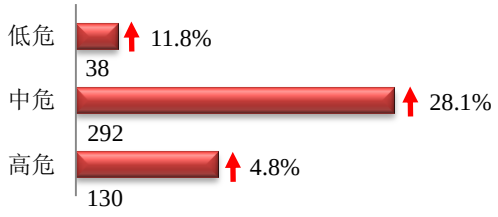


本周我国境内被植入后门网站按类型分布
(3/12-3/18)

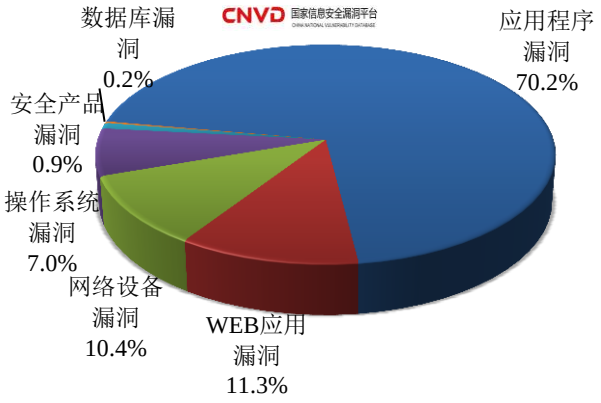


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 460 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
(3/12-3/18)



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

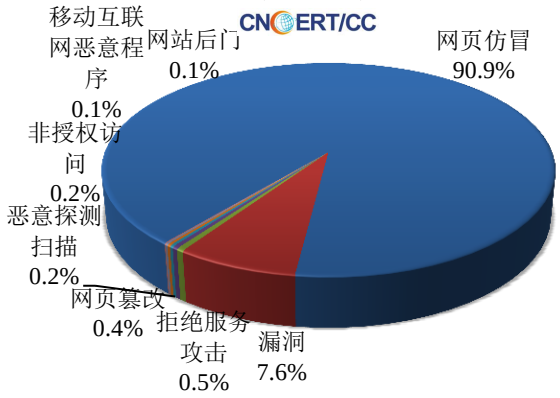
http://www.cnvd.org.cn/webinfo/list?type=4

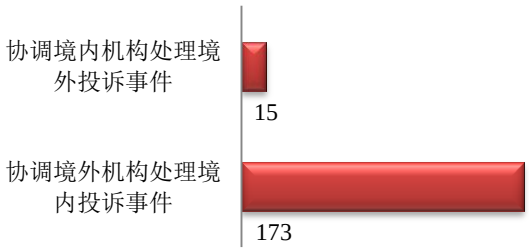
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 846 起，其中跨境网络安全事件 188 起。

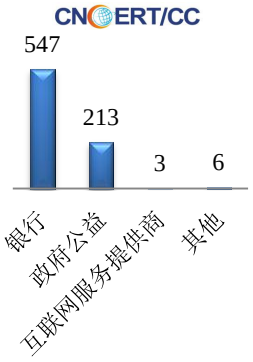
本周CNCERT处理的事件数量按类型分布
(3/12-3/18)



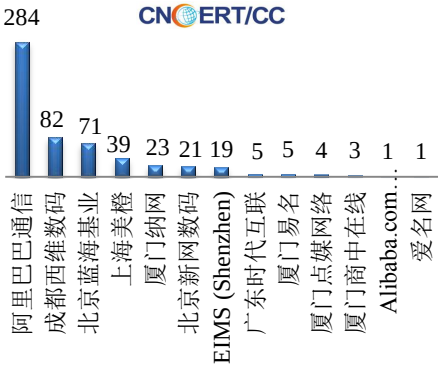


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 769 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 547 起和政府公益仿冒事件 213 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计(3/12-3/18)

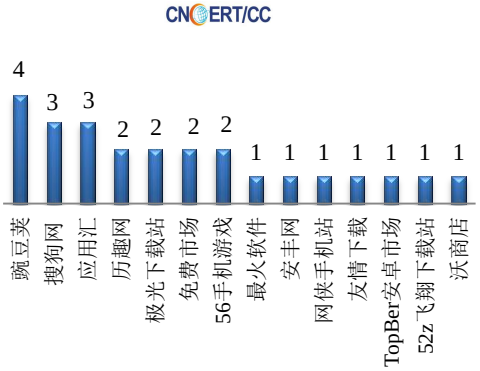


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (3/12-3/18)



本周，CNCERT 协调 14 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 25 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 (3/12-3/18)



业界新闻速递

1、美 35 个州及哥伦比亚特区决定自行立法或签署行政命令保护“网络中立”

cnBeta.COM3 月 18 日消息 据外媒报道，本周，加利福尼亚州提出一项保留“网络中立”的法案，它的全面性甚至可能会压倒美联邦通信委员会（FCC）最近采取的保护措施。推出法案是美国各州反抗 FCC 去年作出的废除“网络中立”决定的唯一方法。据 Fight for the Future 组织统计，目前已经有 35 个州以及哥伦比亚特区为此作出了努力，当中就包括了自行立法和通过颁布行政命令保护“网络中立”。由于这些州不得不面临如何绕过 FCC 在通过废除“网络中立”时做的各州不得自行立法的规定的障碍，所以当它们最终通过自己的“网络中立”法将势必会面临法律诉讼。于是为了避开这一雷区，一些州选择通过签署行政命令来达到保护“网络中立”

的目的。目前还不清楚究竟最终哪些法律会通过，但作为首个通过“网络中立”法的州，华盛顿州看起来已经准备好在法庭跟 FCC 抗争了。

2、俄中选委网站遭到黑客攻击 攻击源来自 15 个国家

环球网 3 月 18 日消息 俄罗斯卫星通讯社莫斯科 3 月 18 日报道称，当地迎来俄罗斯总统选举日，莫斯科市及莫斯科州的所有投票站于当地时间 8 点开放。卫星网 18 日报道称，当日，俄罗斯中央选举委员会发现其网站遭到 DDOS 攻击，攻击源来自 15 个国家。此前，俄罗斯电信公司负责人米哈伊尔·奥谢叶夫斯基 17 日表示，在俄罗斯大选前夕黑客的攻击出现增加，特别是对俄罗斯联邦通信、信息技术和大众传媒监督局网站的攻击。

3、恶意软件攻击沙特阿拉伯石油工厂 试图引发爆炸

cnBeta.COM3 月 16 日消息 沙特阿拉伯一家石油化工企业于 8 月份在工厂发现的恶意软件旨在破坏设备，并可能导致爆炸，从而摧毁整个工厂。据调查人员表示，攻击失败的唯一原因是由于导致系统关闭的违规代码存在缺陷。如果恶意软件被正确写入，那么现有的石油设施就会减少一个。相信政治动机可能是这种攻击的原因，由于攻击代码的复杂性，相信背后有敌对政府支持。由于整个行业使用相同的工业控制器，因此担心可能会对其他化学加工设施发起相同的攻击。软件分析显示，迄今尚未在任何其他系统上发现使用的代码。为了设计使用的恶意软件，开发人员能够提前访问 Triconex 安全系统组件以进行测试几乎是必不可少的。调查人员表示，所需零件在 eBay 上的价格约为 4 万美元。美国政府实体和私人安全公司 Mandiant 仍然在处理这一事件。国家安全局，联邦调查局，国土安全部以及国防高级研究计划局（DARPA）都在努力收集尽可能多的信息。虽然关于攻击实际如何工作的信息很少，但相信恶意代码可以被远程注入，从而使得另一次攻击的威胁很高。

4、远程桌面协议 CredSSP 出现漏洞，影响所有版本的 Windows

HackerNews.cc3 月 14 日消息 RDP 和 WInRM 中使用的 CredSSP 协议（安全加密 Windows 用户远程登录过程）中出现严重漏洞，影响所有版本的 Windows。远程攻击者可以利用这个漏洞，使用 RDP 和 WinRM 窃取数据并运行恶意代码。这个漏洞由网络安全公司 Preempt Security 发现，编号为 CVE-2018-0886，是一个逻辑加密漏洞，可被中间人攻击者利用，通过 WiFi 或物理接触网络来窃取 session 认证数据，发起远程进程调用攻击。如果用户和服务器通过 RDP 和 WinRM 连接协议进行认证，中间人攻击就能执行远程命令，入侵企业网络。而由于 RDP 是远程登录中最常用的应用，几乎所有企业用户都在使用，因此，这个漏洞可造成大范围影响。目前，微软已经发布相关更新补丁，用户应尽快下载更新，同时可以禁用 RDP 等相关应用端口，尽可能少使用特权账户，多使用非特权账户。

5、美研究人员发现 4G 网络多个新漏洞

新华网 3 月 18 日消息 美国研究人员最近发现 4G-LTE 网络的 10 个新漏洞，可能被攻击者用来群发假消息，还可能致使服务器瘫痪。LTE 是“长期演进”的简称，是 4G 网络技术的一种。美国珀杜大学日前宣布，该校研究人员和艾奥瓦大学同行使用了一种叫作“LTE 检查者”的工具，发现了 4G-LTE 网络中的这些漏洞。研究人员表示，这种工具首次能对 4G-LTE 网络中的“连接”“断开”“寻呼”等过程进行系统性分析。研究人员说，利用这些漏洞可以发起多种形式的攻击，能够绑架目标设备的寻呼信道、向大量设备群发伪造的紧急信息、强

迫设备执行某些操作以耗尽其电量，还可阻断设备与核心网的连接等。此外，这些漏洞还能让攻击者无须认证就可接入核心网，在获得用户地址信息后发起“拒绝服务攻击”，导致服务器瘫痪。研究人员实测了 10 个新漏洞中的 8 个，证明修复它们并非易事。在不破坏“向下兼容”的条件下给现有系统“打补丁”，难以阻止极端条件下的攻击。要解决相关问题，可能需要重新调整 4G-LTE 网络的整体架构。研究人员呼吁设备制造商和网络供应商展开合作，对 4G-LTE 网络整个系统进行更新，以堵住这些漏洞。

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