国家互联网应急中心

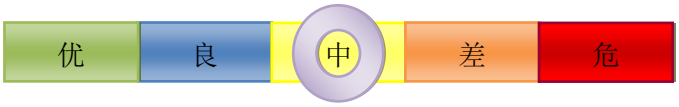
网络安全信息与动态周报

2019 年第 46 期

11 月 11 日-11 月 17 日

CNCERT/CC

本周网络安全基本态势

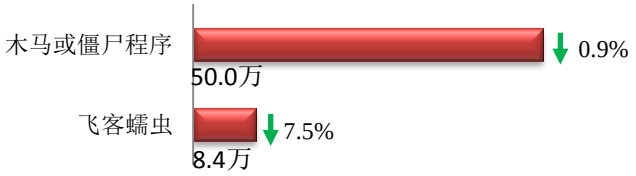


境内感染网络病毒的主机数量	•58.43万	1.9%
境内被篡改网站总数 其中政府网站数量	•8682 •19	36.0% 90.0%
境内被植入后门网站总数 其中政府网站数量	•2989 •61	11.2% 29.8%
针对境内网站的仿冒页面数量	•353	42.5%
新增信息安全漏洞数量 其中高危漏洞数量	•541 •142	27.3% 35.2%

=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

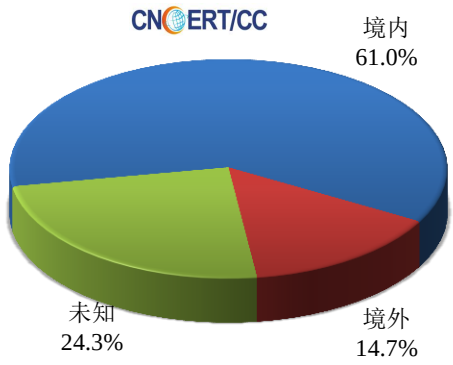
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 58.4 万个，其中包括境内被木马或被僵尸程序控制的主机约 50.0 万以及境内感染飞客（conficker）蠕虫的主机约 8.4 万。

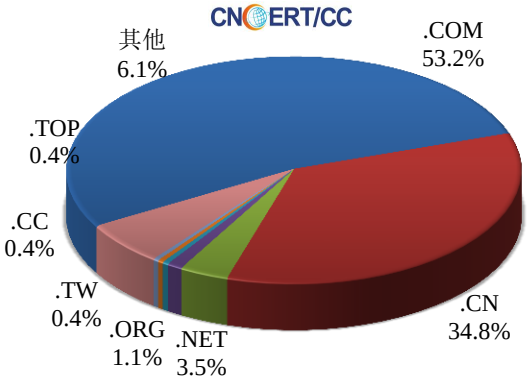


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 2985 个，涉及 IP 地 2625 个。在 2985 个域名中，有 14.7%为境外注册，且顶级域为.com 的约占 53.2%；在 2625 个 IP 中，有约 41.2%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 355 个 IP。

本周放马站点域名注册所属境内外分布
(11/11-11/17)



本周放马站点域名所属顶级域的分布
(11/11-11/17)



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。

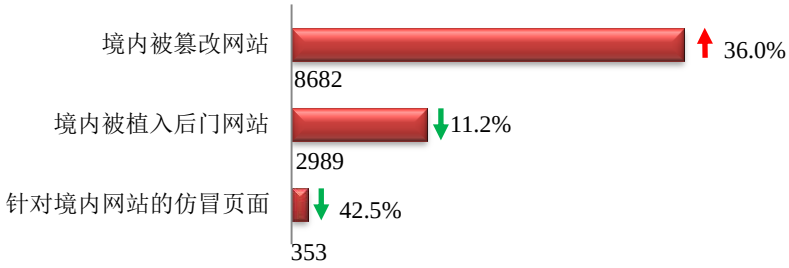
ANVA恶意地址黑名单发布地址

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。

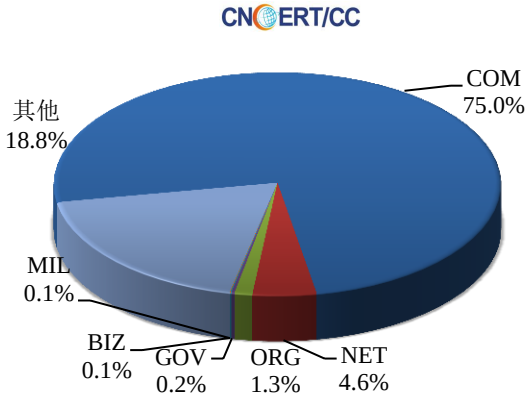
本周网站安全情况

本周 CNCERT 监测发现境内境内被篡改网站数量 8682 个；被植入后门的网站数量为 2989 个；针对境内网站的仿冒页面数量 353 个。

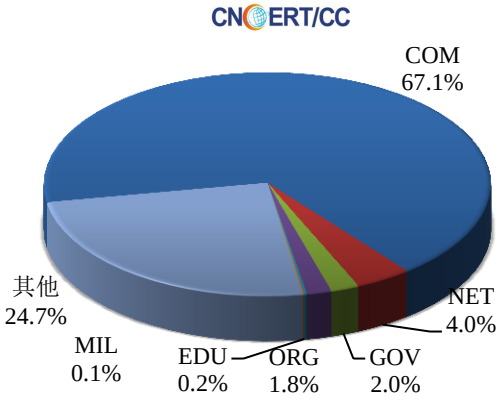


本周境内被篡改政府网站（GOV 类）数量为 19 个（约占境内 0.2%），较上周环比上涨了 90.0%；境内被植入后门的政府网站（GOV 类）数量为 61 个（约占境内 2.0%），较上周环比上涨 29.8%；针对境内网站的仿冒页面涉及域名 219 个，IP 地址 127 个，平均每个 IP 地址承载了约 3 个仿冒页面。

本周我国境内篡改网站按类型分布
(11/11-11/17)

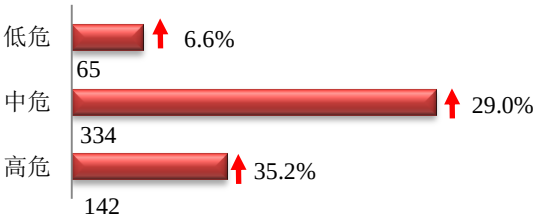


本周我国境内被植入后门网站按类型分布
(11/11-11/17)

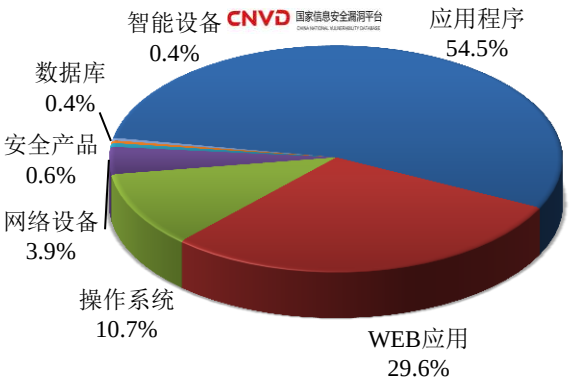


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 541 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
(11/11-11/17)



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 应用漏洞和操作系统。

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

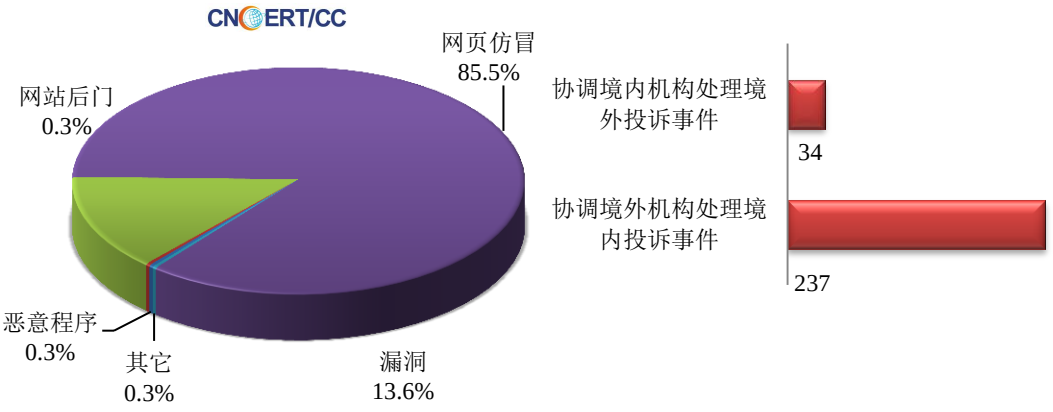
http://www.cnvd.org.cn/webinfo/list?type=4

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

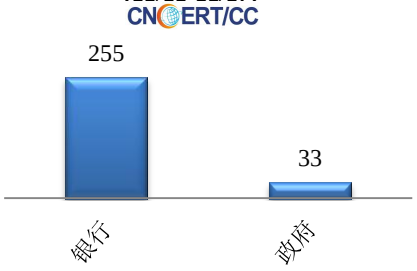
本周，CNCERT 协调基础电信运营企业、域名注册服务机构、手机应用商店、各省分中心以及国际合作组织共处理了网络安全事件 337 起，其中跨境网络安全事件 271 起。

本周CNCERT处理的事件数量按类型分布 (11/11-11/17)

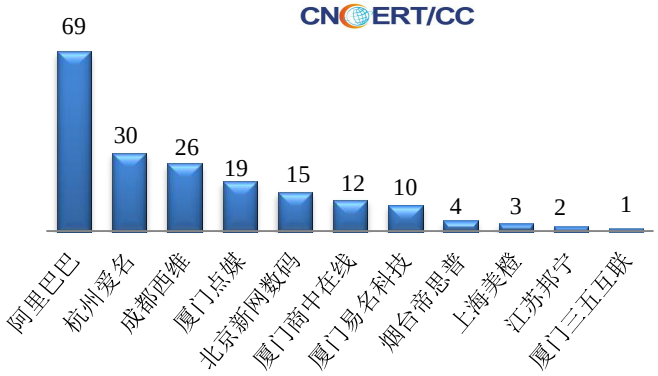


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 288 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，银行仿冒事件 255 起和政府网站事件 33 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (11/11-11/17)

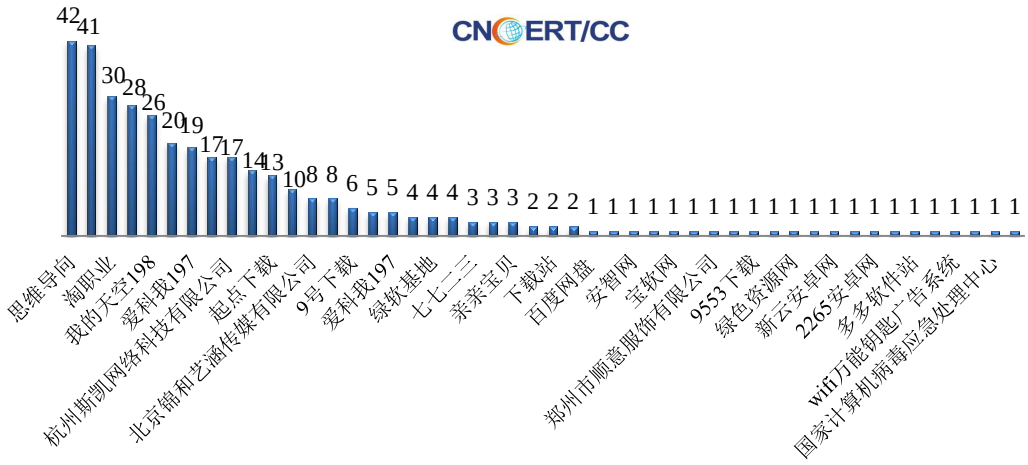


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (11/11-11/17)



本周，CNCERT 协调 48 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 358 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
(11/11-11/17)



业界新闻速递

1、 中国互联网金融协会发布关于加强个人信息保护意识依法开展业务的通知

11 月 11 日，21 世纪经济报道，中国互联网金融协会于 11 月 6 日向其会员单位下发《关于增强个人信息保护意识依法开展业务的通知》。中国互联网金融协会指出，根据国家监管部门发现，社会上有一些互联网机构以“大数据”为名，通过“爬虫”业务涉嫌违法违规收集个人信息，或窃取、滥用、买卖、泄露个人信息，侵犯了消费者个人隐私，造成了不良的社会影响。为此，中国互联网金融协会要求，不与违规收集和使用个人信息的第三方开展数据合作，不滥用、非法买卖和泄露消费者个人信息。同日，北京地区部分互联网金融机构收到监管要求全面停止与“爬虫”有关的放贷业务，导致一些平台的基于“爬虫”的放贷业务全面暂停。诞生于搜索引擎时代的网络爬虫，在个人信息保护意识增强的当下，正在受到监管和法律的关注。

2、 托管提供商 SmarterASP.NET 承认遭到勒索软件攻击客户数据被加密

11 月 12 日 CNBeta 网站消息，SmarterASP.NET 公司发布公告称遭到勒索软件的攻击，这也是 2019 年遭到网络攻击而下线的第三家大型网络托管公司，黑客不仅破坏了攻击的托管业务而且还对客户服务器上的数据进行了加密。SmarterASP.NET 官方表示正在努力恢复客户数据，但尚不清楚该公司是支付了赎金，还是从备份中进行了恢复。

3、 字节码联盟成立，WebAssembly 生态将完善网络安全性

11 月 13 日，外媒 Techcrunch 消息，Mozilla、Fastly、Intel 与 Red Hat 宣布成立联合组织 Bytecode Alliance（字节码联盟），该联盟旨在通过协作实施标准和提出新标准，以完善 WebAssembly 在浏览器之外的生态。消息指出，Bytecode Alliance 将建立起可靠安全的基础，无论在云中、本地桌面，还是小型 IoT 设备上，都可以安全地使用不受信任的代码。开发人员可以以相同的方式使用开源代码，而不会给用户带来风险，而这些通用的可重用基础集可以单独使用，也可以嵌入其它库和应用中。

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 2018 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：徐原

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315