国家互联网应急中心

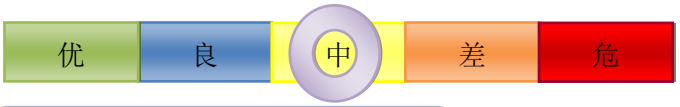
网络安全信息与动态周报

2019 年第 44 期

10 月 28 日-11 月 3 日

CNCERT/CC

本周网络安全基本态势

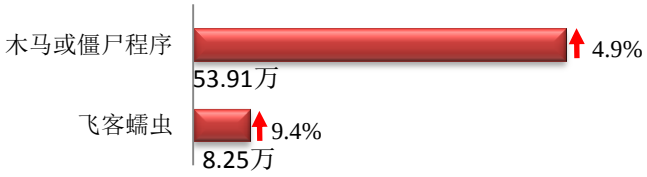


境内感染网络病毒的主机数量	•62.16 万	↑5.5%
境内被植入后门网站总数 其中政府网站数量	•2975 •73	↓4.6% ↑128.1%
针对境内网站的仿冒页面数量	•1884	↑229.4%
新增信息安全漏洞数量 其中高危漏洞数量	•478 •92	↓0.2% ↓26.4%

=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

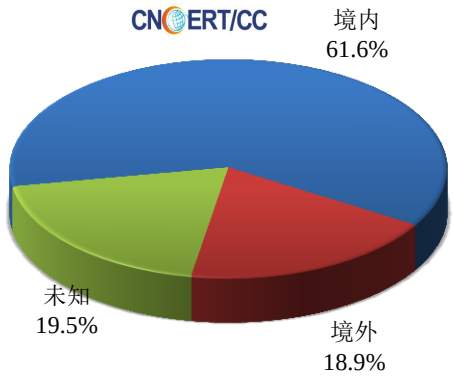
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 62.16 万个，其中包括境内被木马或被僵尸程序控制的主机约 53.91 万以及境内感染飞客（conficker）蠕虫的主机约 8.25 万。

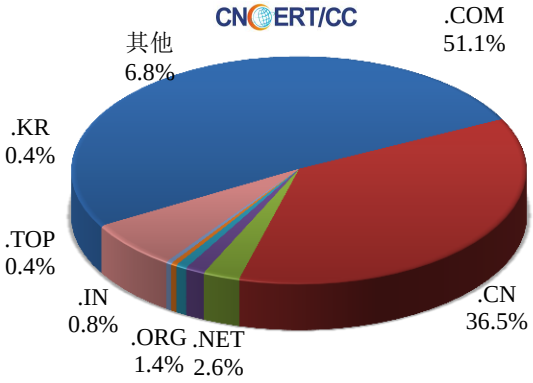


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域 3291 个，涉及 IP 地 2712 个。在 3291 个域名中，有 18.9%为境外注册，且顶级域为.com 的约占 51.1%；在 2712 个 IP 中，有约 45.9%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 414 个 IP。

本周放马站点域名注册所属境内外分布
(10/28-11/3)



本周放马站点域名所属顶级域的分布
(10/28-11/3)



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。

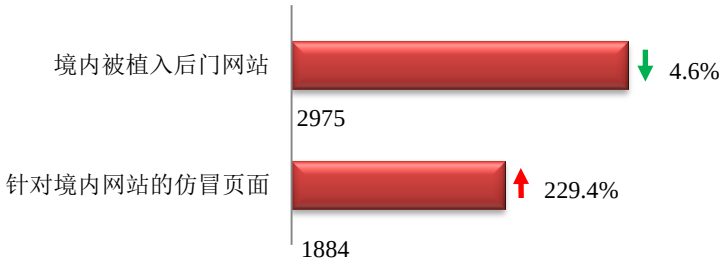
ANVA恶意地址黑名单发布地址

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。

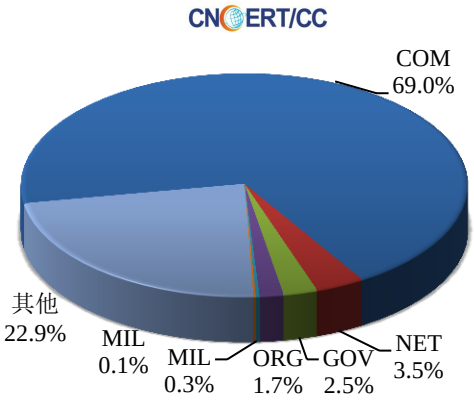
本周网站安全情况

本周 CNCERT 监测发现境内被植入后门的网站数量为 2975 个；针对境内网站的仿冒页面数量 1884 个。篡改网站数量 6627 个，其中 GOV 类 17 个。



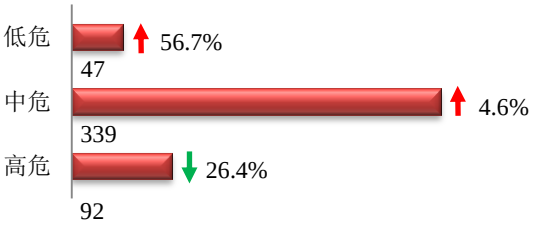
本周境内境内被植入后门的政府网站（GOV 类）数量为 73 个（约占境内 2.5%），较上周环比上涨 128.1%；针对境内网站的仿冒页面涉及域名 1145 个，IP 地址 385 个，平均每个 IP 地址承载了约 5 个仿冒页面。

本周我国境内被植入后门网站按类型分布
(10/28-11/3)

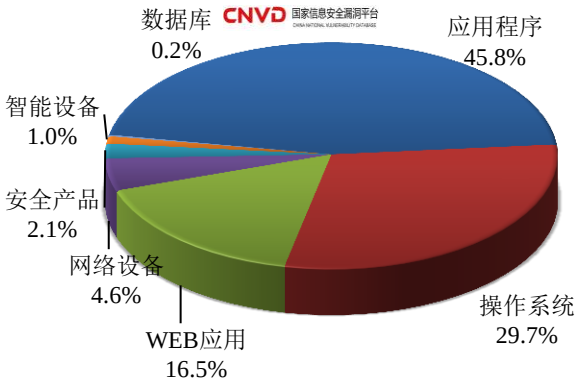


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 478 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
(10/28-11/3)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是操作系统和 WEB 应用漏洞。

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

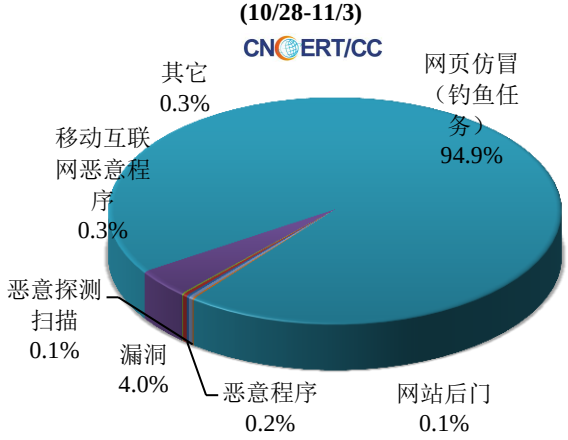
http://www.cnvd.org.cn/webinfo/list?type=4

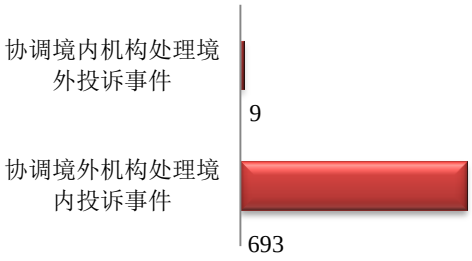
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信运营商、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

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 1347 起，其中跨境网络安全事件 702 起。

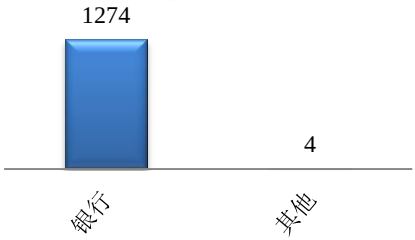
本周CNCERT处理的事件数量按类型分布
(10/28-11/3)



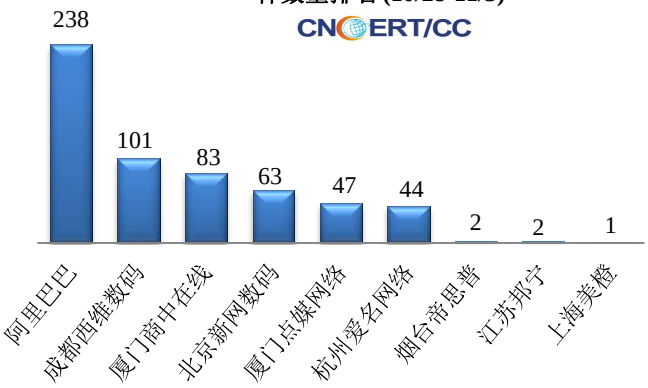


本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 1278 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，主要包含银行仿冒事件 1274 起和其他仿冒事件 4 起。

本周CNCERT处理网页仿冒事件数量按仿冒对象涉及行业统计 (10/28-11/3)

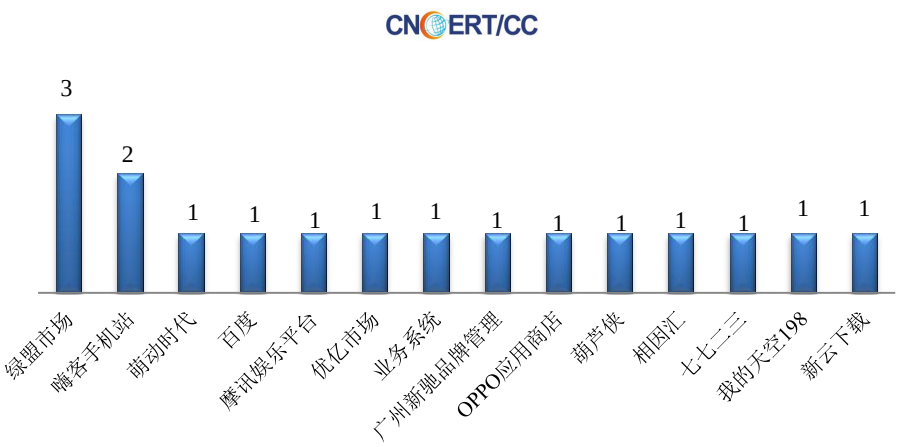


本周CNCERT协调境内域名注册机构处理网页仿冒事件数量排名 (10/28-11/3)



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 17 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 (10/28-11/3)



业界新闻速递

1、 美国 NIST 发布《大数据互操作框架》最终版

10 月 29 日美国“NIST”网站消息，美国国家标准与技术研究院（NIST）发布了《大数据互操作框架》的最终版本。该框架共 9 卷，由 NIST 与来自行业、学术界、政府的

800 多名专家合作制定，旨在改进大数据分析方法。该框架确定了一致的定义和分类法，以帮助开发人员在讨论新工具的计划时保持一致。它还包括这些工具应该具备的数据安全和隐私保护的关键要求，并新增了参考性的架构接口规范，用于指导这些工具的实际部署。这一规范将指导开发人员部署可以使用任何类型的计算平台分析数据的软件工具，还将使供应商能够构建任何工具都可在其中运行的灵活环境。它还允许分析人员将他们的工作从一个平台转移到另一个平台，并替换一个更高级的算法，而无需重新配置计算环境。

2、 波兰总理批准《波兰网络安全战略（2019-2024）》

10 月 29 日波兰“Polandin”网站消息，波兰数字化部近日宣布，为了适应新形势下的网络安全需求，确保云安全和 5G 等网络安全，波兰总理马泰乌什•莫拉维茨基批准了《波兰网络安全战略（2019-2024）》。该战略旨在改进波兰的网络弹性，并更好地保护公私部门及军事系统的数据。战略确定了 5 个具体目标：第一，开发国家网络安全系统（KSC），评估系统功能；第二，改进政府机构和私营部门的网络弹性，将网络安全事件的影响降至最低；第三，提高波兰在网络安全技术领域的潜能，建立公私部门之间的合作机制；第四，提升全社会的网络安全意识和网络安全事件处置人员的专业技能；第五，增强波兰在国际网络安全领域的地位，积极开展技术、操作等层面的国际合作。

3、 浣熊恶意软件感染全球数十万设备窃取信息

10 月 28 日 cybereason 消息，浣熊恶意程序（Raccoon）是一种恶意软件即服务（MaaS）信息窃取程序，于 2019 年初出现，并于 2019 年 4 月开始在互联网地下黑色产业链论坛上积极销售。此后，其在互联网地下黑色产业链中使用量急剧增加。它已成为互联网地下黑色产业链十大最受引用的恶意软件之一，并感染了北美、欧洲、亚洲的个人和组织的数十万个端点。恶意软件注册表配置有 30 多种不同的目标浏览器包括（360 浏览器、火狐浏览器），从目标浏览器中窃取 cookie 和自动填充数据。

4、 15000 个网站被破坏，格鲁吉亚遭受该国史上最大规模网络攻击

10 月 28 日 BBC 消息,格鲁吉亚近期遭受了大规模的网络攻击，超过 15000 个网站被破坏，随后被迫关闭。这次安全事件被当地媒体认为是该国历史上最大规模的网络袭击，影响了多家政府机构、银行、法院、当地报纸和电视台的网站。当地网络托管商 Pro-Service 已出面承担责任，承认是一名黑客侵入了公司网络，瘫痪了旗下大量客户的网站，造成整个国家网络的“宕机”。发言人表示，网络攻击发生在清晨，到当地时间晚上 8 点，工作人员已经恢复了一半以上受影响的网站。

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：常霞

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315