国家互联网应急中心

网络安全信息与动态周报

2018 年第 7 期

2 月 12 日-2 月 18 日

CNCERT/CC

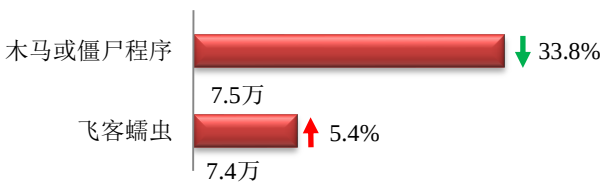
本周网络安全基本态势

境内感染网络病毒的主机数量	• 14.9万	↓ 18.8%
境内被篡改网站总数 其中政府网站数量	• 1957 • 34	↑ 4.9% ↑ 21.4%
境内被植入后门网站总数 其中政府网站数量	• 405 • 5	↓ 43.5% ↓ 44.4%
针对境内网站的仿冒页面数量	• 46	↓ 75.4%

= 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

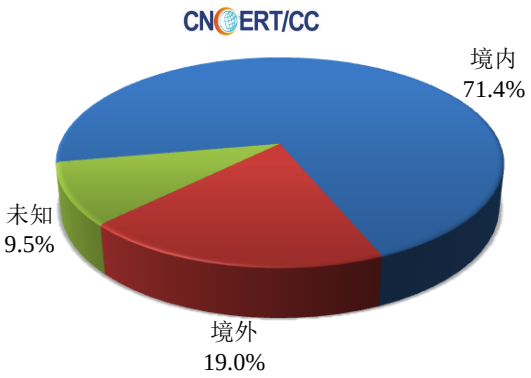
本周网络病毒活动情况

本周境内感染网络病毒的主机数量约为 14.9 万个，其中包括境内被木马或被僵尸程序控制的主机约 7.5 万以及境内感染飞客（conficker）蠕虫的主机约 7.4 万。

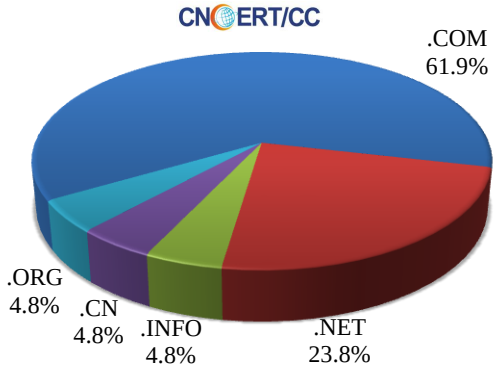


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 21 个，涉及 IP 地址 54 个。在 21 个域名中，有 19.0%为境外注册，且顶级域为.com 的约占 61.9%；在 54 个 IP 中，有约 33.3%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 1 个 IP。

本周放马站点域名注册所属境内外分布
(2/12-2/18)



本周放马站点域名所属顶级域的分布
(2/12-2/18)



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。

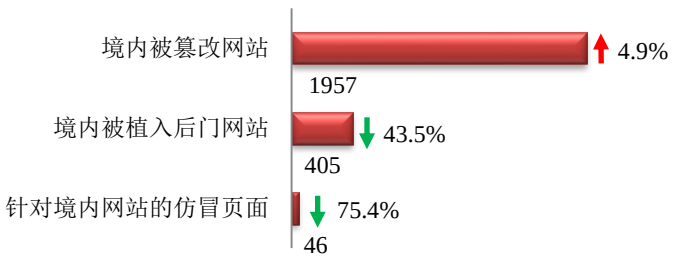
ANVA恶意地址黑名单发布地址

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。

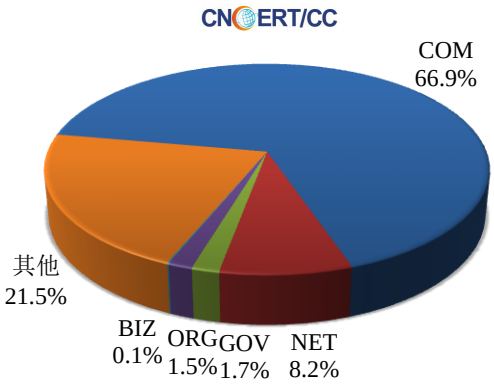
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量为 1957 个；境内被植入后门的网站数量为 405 个；针对境内网站的仿冒页面数量为 46。

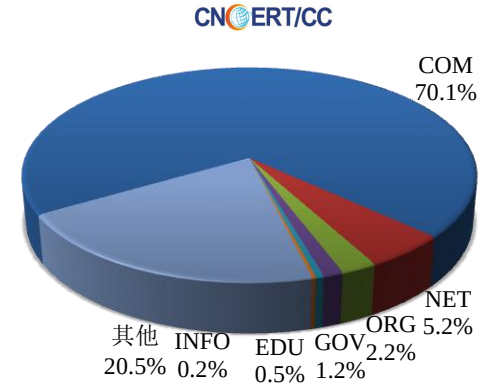


本周境内被篡改政府网站（GOV 类）数量为 34 个（约占境内 1.7%），较上周环比上升了 21.4%；境内被植入后门的政府网站（GOV 类）数量为 5 个（约占境内 1.2%），较上周环比下降了 44.4%；针对境内网站的仿冒页面涉及域名 36 个，IP 地址 24 个，平均每个 IP 地址承载了约 2 个仿冒页面。

本周我国境内被篡改网站按类型分布
(2/12-2/18)



本周我国境内被植入后门网站按类型分布
(2/12-2/18)



业界新闻速递

1、美国与乌克兰开展大规模网络安全合作

E 安全 2 月 16 日消息 上周三（2018 年 2 月 7 日）晚上，美国众议院通过了一项旨在促进美乌政府进一步加强网络安全合作的法案。2017 年，新闻曾曝光乌克兰首都基辅因遭受复杂网络攻击出现大规模断电，仅在三个月后，美国议员代表 Brendan Boyle（宾夕法尼亚州代表）便于 2017 年 4 月首次引入《2017 年乌克兰网络安全协作法案》。此法案的共同发起人是议员 Brian Fitzpatrick（宾夕法尼亚州代表）。法案在众议院获得 404 张赞同票。由于获得了重要的数字防御优先权，包括美国承诺在有需要的时候支持乌克兰政府，所以该法案将推动美国与乌克兰的进一步合作。此法授权国务院发起并组织双方合作，包括向国会定期报告合作的有效性。虽然美国与乌克兰已经在多项外交任务中合作，但是《乌克兰网络安全协作法案》明确要求美国需协助向基辅的政府电脑提供高级安全保护，特别是那些保护乌克兰关键基础设施的系统；向乌克兰提供支持，减少对俄罗斯技术的依赖；帮助乌克兰扩大网络安全信息共享的能力，协作做出国际响应。

2、新加坡三读通过《网络安全法案》

中国信息产业网 2 月 12 日消息 新加坡国会 2 月 5 日三读通过《网络安全法案》（下称《法案》），加强新加坡 11 个关键信息基础设施应对网络袭击的能力，授权网络安全局预防和应对网安事故及制定网安服务提供者的管制框架。根据《法案》，网络安全局在调查网络安全威胁和事故时，有权获取关键信息基础设施的网安信息。通讯及新闻部长雅国在二读阐述《法案》要旨时指出：“政府迫切需要更积极与关键信息基础设施拥有者一起抵

御网络袭击。”雅国称，原有的《滥用电脑和网络安全法令》只应对未经授权使用电脑资料等网络犯罪，没有常规和主动保护关键信息基础设施的管制框架，因此必须授权让网安局对网络安全威胁展开调查，以减缓网络袭击造成的冲击。《法案》明确了 11 个关键信息基础设施领域，包括能源、水资源、银行、金融、医疗保健、海陆空交通、信息通信、媒体、安全、紧急服务和政府。政府是在咨询各领域监管单位和潜在的关键信息基础设施拥有者后，确定了这些关键领域。《法案》要求关键信息基础设施拥有者遵从相应义务，确保他们各自所属基础设施的网络安全，包括及时通报网络安全事故及进行网络安全审查和风险评估等。如果违例，拥有者最多可被判罚 10 万新元，判监两年，或两者兼施。但雅国强调，只要拥有者履行应遵循的义务，就不会因网络遭入侵而被指控。

3、英美政府网站被植入恶意软件：电脑被迫挖掘“门罗币”

凤凰网 2 月 12 日消息 据外媒 The Register 报道，包括英国和美国政府机构在内的数千家网站都在周日被一组恶意代码感染，时间长达数小时，导致感染的电脑开始秘密挖掘数字加密货币。The Register 称，共有 4200 多个网站感染了该恶意软件，这款恶意软件是英国软件公司 Texthelp 公司开发的 Browsealoud 工具的恶意版本，这款工具原本的目的是为有视觉问题的人朗读网页内容。据悉，访问受感染网站的电脑会被迫运行专门挖掘“门罗币”的软件，从而为幕后黑客谋取利益。Texthelp 表示，为了制止这一黑客活动，他们已经停用 Browsealoud，该公司的工程团队也展开了调查。

4、SWIFT 再爆黑客袭击 俄罗斯银行被盗 600 万美元

新浪网 2 月 16 日消息 近年来，SWIFT 系统（环球同业银行金融电讯协会）的全球银行客户不断被爆出遭黑客袭击、账户存款被窃取事件。俄罗斯央行近日披露，该国银行的 SWIFT 系统去年也被黑。据路透社报道，俄罗斯央行周五（2 月 16 日）称，未知黑客在去年对俄罗斯 SWIFT 国际支付信息系统的一次袭击中成功窃取了 3.395 亿卢布（约 600 万美元）。这一信息被放在俄罗斯央行报告中有关数字盗窃部分的最后。俄罗斯央行表示，它之前收到了一条有关“在一个 SWIFT 系统操作员的工作地点成功（发动）袭击”的信息。“这次攻击导致未经批准的操作（金额）达到 3.395 亿卢布。”俄罗斯央行称。俄罗斯央行的披露是全球范围内最新一起黑客袭击 SWIFT 系统并成功窃取银行资金的事件。

5、官员确认平昌冬奥会开幕式期间遭到网络黑客攻击

凤凰网 2 月 12 日消息 援引路透社报道，平昌冬奥会组织者已经证实在开幕式当天遭到网络攻击，但拒绝透露攻击者的相关信息。包括冬奥会网站、电视服务在内均遭到黑客攻击，但是没有造成太过严重的影响，周五主新闻中心的 IPTV 突然黑屏，网络访问和 WiFi 关闭，与会者无法打印门票，直到周六才恢复正常。国际奥委会发言人马克·亚当斯（Mark Adams）说：“我们不会对这个（网络攻击）问题发表置评。这是我们正在解决的问题。我们正在确保我们的系统安全。”上月，McAfee 就曾表示公司在过去数月中已经检测到多次针对冬奥会的网络攻击，主要通过恶意邮件的方式。网络安全专家吉姆·路易斯（Jim Lewis）告诉 CBS 说，黑客以前也经常瞄准奥运会。

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：李志辉

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990158