**2017年第35期**

**8月21日-8月27日**

网络安全信息与动态周报

**国家互联网应急中心**



**本周网络安全基本态势**

良

中

差

危

优

9.7%

7.5%

26.1%

38.8%

20.0%

1.0%

6.6%

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*

****

本周境内感染网络病毒的主机数量包括境内被木马或被僵尸程序控制的主机28.9万以及境内感染飞客（conficker）蠕虫的主机87.3万。

**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57.3万个，其中包括境内被木马或被僵尸程序控制的主机约42.0万以及境内感染飞客（conficker）蠕虫的主机约15.3万。

8.7%

5.0%

**﹦**

1

本周CNCERT捕获的新增网络病毒文件，按网络病毒名称统计新增1个，按网络病毒家族统计无新增。

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59个，涉及IP地址329个。在59个域名中，有28.8%为境外注册，且顶级域为.com的约占74.6%；在329个IP中，有约4.9%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2个IP。

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。

<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**

26.1%

7.5%

6.6%

本周境内被篡改政府网站（GOV类）数量为44个（约占境内2.0%），较上周环比下降了20.0%；境内被植入后门的政府网站（GOV类）数量为65个（约占境内5.9%），较上周环比下降了9.7%；针对境内网站的仿冒页面涉及域名272个，IP地址116个，平均每个IP地址承载了约3个仿冒页面。

本周CNCERT监测发现境内被篡改网站数量为2184个；境内被植入后门的网站数量为1109个；针对境内网站的仿冒页面数量为325。

**本周重要漏洞情况**

38.8%

18.2%

17.6%

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞292个，信息安全漏洞威胁整体评价级别为中。

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。

<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794起，其中跨境网络安全事件369起。

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701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649起和互联网服务提供商仿冒事件40起。

本周，CNCERT协调11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42个。

**业界新闻速递**

**1、**[**国家网络安全学院项目武汉开建**](http://cnews.chinadaily.com.cn/2017-08/24/content_31036690.htm)

中国日报网8月24日消息 国家网络安全学院及配套的超算数据中心、科技孵化园等一批项目8月23日在武汉市临空港经济技术开发区集中开工建设。项目总投资达到216亿元。这标志着由中央网信办扶持的首个“国家网络安全人才与创新基地”整体进入实质性建设阶段。国家网络安全学院项目总用地面积1500亩，总投资50亿元，规划建设网络安全学院、培训学院和研究院。项目计划2018年11月完成结构封顶，2019年6月建成投入运营，将为1万人提供教育培养和专业培训的学习研究及生活的场所，为打造网络安全人才提供重要载体。与国家网络安全学院项目配套的展示中心、国际人才社区、超算数据中心等一批项目当日也同步开工建设。

**2、**[**美国家基础设施顾问委员会警告防范“911”网络攻击**](https://www.easyaq.com/news/1786486210.shtml)

E安全8月24日消息 美国国家基础设施顾问委员会（简称NIAC）周二通过的一份报告，指出美国处于911前的紧迫时刻，在大型攻击到来之前，美国必须抓住稍纵即逝的微小机会有效协调资源。报告警告称，美国未做好准备应对针对电网、通信系统等关键基础设施的灾难性网络攻击。顾问委员会成员包括公司高管和前政府高级官员投票通过这份报告，建议美国建立独立的通信网络以支持关键系统，并采取措施解密网络安全威胁信息，以便前线基础设施运营商可利用这些信息防御攻击。报告提到的建议措施包括，强化劳动力、改进机器对机器信息共享并简化安全调查程序，从而消除私有部门和承包商担负的不对称工作积压。NIAC建议由白宫国家安全顾问监督关键基础设施网络安全，此外还提到能源部的公共/私有网络安全风险信息共享计划和国土安全部网络信息共享与合作计划。报告指出，当美国基础设施遭遇国家攻击时，私营企业在网络中处于防御第一线。

**3、**[**亚马逊AWS服务器信息泄露 180万选民信息曝光**](http://tech.sina.com.cn/i/2017-08-21/doc-ifykcypq1590487.shtml)

新浪网8月21日消息 北京时间8月21日早间消息，美国一家选票计算机公司上周四证实，他们泄露了180多万伊利诺伊州居民的个人信息。该公司已经上报伊利诺伊州政府和美国联邦调查局（FBI），而泄露的信息中包含选民姓名、地址、出生日期、部分社会安全号和部分党派关系，此外还包含一些驾驶执照和州身份证信息。网络安全公司UpGuard的乔·亨得利（Jon Hendren）在一台未受密码保护的亚马逊网络服务（AWS）设备上发现了此项漏洞。磁盘分析师克里斯·维客利（Chris Vickery）随后下载了这些选票数据，并判断这些数据来自Election Systems & Software（以下简称“ES&S”）——这家公司为至少42个州提供选票计算机和服务。ES&S在声明中表示，该公司也已经在UpGuard的协助下自行展开“彻底调查”。该公司称，AWS服务器并未包含任何投票信息，也不会对任何选举结果产生影响。

**4、**[**黑客使用.fish域名网站来骗取法国银行客户**](http://www.cnbeta.com/articles/tech/644017.htm)

[cnBeta.COM](http://www.cnbeta.com/)8月22日消息 网络安全公司Netcraft发现黑客使用.fish域名网站来骗取法国银行客户，他们发现一个采用.fish域名的网站伪装成法国银行网站来对客户进行钓鱼攻击。当有人访问parser.fish时，他们将被重定向到一个越南网站，伪装成法国银行BRED，同时试图盗取用户的银行证书。经过查他们发现，Parser.fish域名在多伦多的托管服务Tucows上匿名注册，这并非不平常，但这就几乎不可能找出谁拥有该网站，以及它是如何被黑掉的，最有可能的解释是该网站遭到黑客入侵。幸运的是，目前该网站已经被清除了恶意代码。.fish成为顶级域名已经有一段时间了。它是几个新顶级域名之一，如.sexy，.tech和.xyz，它们和地理位置没有关系，.fish顶级域名主要针对那些对水生生物感兴趣的用户。

**5、**[**维基解密：CIA利用虚假软件升级系统来监控合作伙伴**](http://tech.ifeng.com/a/20170825/44668015_0.shtml)

凤凰网8月25日消息 据科技博客The Verge北京时间8月25日报道，维基解密今天公布的一份文件显示，美国中央情报局（CIA）曾秘密创建了一个虚假的软件更新系统，用以暗中监视情报合作伙伴，而这一秘密项目最早可以追溯到2009年。这一秘密项目名为“ExpressLane”，该项目与CIA的生物识别系统一道被CIA部署给合作机构。理论上来讲，只有经这些合作伙伴同意，CIA才能够访问特定的生物识别数据，但在秘密部署“ExpressLane”项目后，CIA能够在合作伙伴不知情的情况下暗中获取相关信息。据悉，“ExpressLane”被伪装成一款软件升级，由CIA技术人员亲自送给合作伙伴。但文件清晰地表明，这个项目本身实质上并未改变系统。相反，该项目能够将系统的数据传输到一个U盘上，供CIA查询使用，从而查看合作伙伴的系统是否设置了障碍。如果合作伙伴拒绝了虚假的更新软件，那么就会有一个隐藏的kill开关启动，让CIA有权在一段时间后关闭整个系统，并需要CIA技术人员亲自访问帮助恢复系统。

**6、**[**加密货币勒索软件Miner可利用WMI与“永恒之蓝”肆意传播**](http://hackernews.cc/archives/13811)

HackerNews.cc8月23日消息 据外媒8月21日报道，趋势科技（Trend Micro）研究人员近期发现加密货币勒索软件Miner，允许黑客利用Windows管理工具WMI与安全漏洞“永恒之蓝（EternalBlue）”进行肆意传播。据悉，该勒索软件首次于今年7月发现，受其影响最严重的国家包括日本（43.05%）、印度尼西亚（21.36%）、台湾（13.67%）、泰国（10.07%）等。研究人员表示，该勒索软件使用WMI作为无文件持久性机制，即由WMI Standard Event Consumer脚本应用程序（scrcons.exe）执行。此外，Miner还使用EternalBlue漏洞感染系统网络。研究显示，无文件WMI脚本与EternalBlue的结合可以使Miner隐蔽持久的感染目标设备。Miner的感染流程分为多个阶段。首先，Miner感染目标系统后会通过EternalBlue漏洞删除并运行系统后门（BKDR\_FORSHARE.A）；其次，系统在安装各种WMI脚本后，会将其连接到C＆C服务器并获取指令；最终，目标系统将下载运行该恶意软件与其相关组件进行肆意传播。

**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。截止2016年，CNCERT与69个国家和地区的185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：张帅

网址：www.cert.org.cn

email：cncert\_report@cert.org.cn

电话：010-82990158