

中国互联网网络安全威胁治理联盟运作机制

一、背景目的

2015 年 7 月 31 日，CNCERT 会同中国互联网协会网络与信息安全工作委员会联合国内 54 家企事业单位通过行业自律方式，启动了互联网网络安全威胁治理专项行动，对拒绝服务攻击、网页暗链篡改等与互联网黑产密切相关的事件进行了重点处置。经过努力，截至 2016 年 1 月 31 日，DDoS 攻击事件日均次数由行动前的 1491 起下降到 265 起，下降了 82.2%，境内被篡改网站月均数量下降 21.4%，被篡改政府网站月均数量下降 56.2%。为持续开展互联网网络安全威胁治理工作，通过成立中国互联网网络安全威胁治理联盟，构建威胁治理联盟体系，加强威胁情报共享和威胁协同处理，有效净化网络安全环境，树立我国负责任网络大国形象。

二、联盟机构

互联网网络安全威胁治理联盟由联盟专家委员会、联盟秘书处和联盟成员单位组成。

联盟专家委员会由互联网行业相关专家组成，主要负责对联盟运行相关工作提供技术支持和专家意见。

联盟秘书处设在 CNCERT，主要负责联盟的日常运行。设秘书长。

联盟成员单位主要负责日常网络安全威胁的举报、共享和处置。

三、工作内容

在联盟框架下，开展对拒绝服务攻击、网页篡改、网站后门、网络钓鱼、隐私窃取、恶意程序、域名安全等网络安全威胁的情报共享和事件协同处置。

四、工作流程

（一） 投诉举报

联盟秘书处设置电话、邮件、在线等多种举报方式，广泛接收社会及联盟成员单位对各类网络安全威胁的投诉举报。

（二） 情报共享

联盟秘书处负责整理通过多种渠道获得的可共享的网络安全威胁情报数据；联盟成员单位可以通过数据接口，获得情报共享。

联盟成员单位可以向联盟秘书处共享自主获得的网络安全威胁情报数据；联盟秘书处对联盟成员单位允许共享他人的网络安全威胁情报进行统一共享。

（三） 威胁认定

联盟秘书处负责对一般网络安全威胁进行直接分析和认定；对于影响范围较大的网络安全威胁，由联盟秘书处提交联盟专家委员会进行研判后认定。

（四） 协同处置

联盟秘书处负责协调联盟成员单位开展对确定要处置的网络安全威胁事件进行处置；联盟成员单位负责对联盟秘书处下发的网络安全威胁处置指令进行处置，并反馈处置结果。处置方式包括但不限于：（1）对网络攻击行为进行记录、分析、溯源；（2）对网络攻击相关的 IP 地址、域名、URL、APP、电子邮箱账号、其它通讯账号等进行积极处置；（3）在终端对恶意 IP 地址、恶意网址、恶意 APP、恶意电话号码等进行拦截或提示；（4）屏蔽网络攻击服务或工具的售卖和推广渠道。

联盟秘书处负责接收申诉者的申诉请求；对一般网络安全威胁处置的申诉请求由联盟秘书处进行直接处理；对于影响范围较大的网络安全威胁处置的申诉请求由联盟秘书处提交联盟专家委员会进行研判，提出处理意见，由联盟秘书处进行具体实施。

（五） 信息发布

联盟秘书处负责定期对网络安全威胁情报、整治情况等进行分析，并以报表、报告、地图等多种方式公开发布。