



## 亚信安全：2016 将是网络勒索之年

*亚信安全发布《2016 信息安全威胁预测报告》：网络威胁日趋精密，  
凸显安全立法与企业网络安全防御必要性*

**【亚信安全】 - 【2015 年 12 月 15 日】** 近日，中国云与大数据的安全技术领导者亚信安全发布了《2016 年信息安全威胁预测报告》。报告指出，2016 将是网络勒索之年，网络勒索集团将会想出更多新的方法来针对个别受害者的心理，每一次的攻击会变得更“个人化”。而激进主义黑客攻击、移动恶意程序在明年也将不断增长，网络不法分子将采取更先进、更具针对性的方式来进行网络攻击。据此，亚信安全建议个人消费者与企业用户要更加重视网络攻击技术的演变，并持续改进网络安全防御措施，以应对不断精进的网络安全威胁。

未来，网络勒索集团将会想出更多新的方法来针对个别受害者的心理，让每一次的攻击变得更「个人化」，不论其目标是特定用户或是某家企业。名誉就是一切，因此能够威胁个人或企业名誉的攻击，不但非常有效，而且最重要的，非常有利可图。

亚信安全董事长何政表示：“2016 年对于网络安全行业来说是非常重要的一年。在网络防护方面，政府将更加重视网络安全法律及政策的制定，越来越多的企业将把网络安全防护作为重要的企业战略。在网络攻击方面，随着用户网络威胁防御意识的不断提升，黑客势必会采取更强烈的攻势，采用更先进、更具针对性的方式来攻击特定目标。但是，正义之士将会看到更多正面的成效，包括更多成功破获网络犯罪的案例，掌握有效提升防御能力的办法，并肩作战、共同进步。”

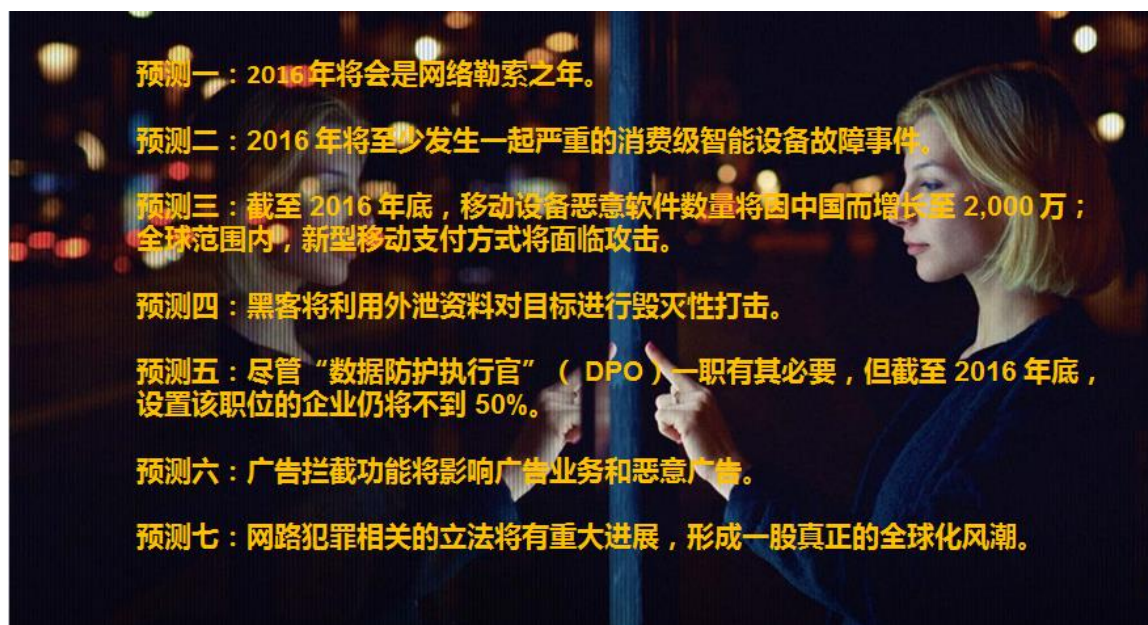
报告指出，2016 年全球网络攻击手段将发生不少新变化，其中恶意广告的转变，以及黑客针对智能设备的攻击将尤为突出。首先，2015 年广告拦截软件在全球使用率增长了 41%，并且在国内具备广告拦截插件功能的浏览器也越来越流行，不法广告商开始尝试其它类型的网络广告推送方式，以谋求绕过拦截软件，例如借助山寨 APP 进行广告推送。其次，2015 年发生多起过智能装置遭到入侵的事件，从婴儿监视器、智能型电视到联网汽车都有，随着

智能联网家用设备“被黑”情况的愈演愈烈，或将促成政府制定法规来约束智能设备的生产与使用。

报告还指出，2016 年将是网络勒索行为大幅度扩展的一年，锁屏（FakeAV）、恐吓型勒索软件、加密型勒索软件会严重影响个人与企业用户信息系统的正常使用。一方面是因为与其它网络犯罪手段相比，网络勒索更有可能帮助不法分子获得高额收益。另一方面，亚信安全也发现，微信等社交网络的应用加速了网络勒索行为的发展，黑客将尽可能通过消费者心理弱点传播恶意软件，造成二次感染，以勒索目标对象。

亚信安全技术部总经理蔡昇钦指出：“在网络攻防中，黑客并非总是会采取固定不变的攻击套路，而是会根据个人消费者及企业的安全防御措施而改变攻击方式。因此，我们可以看到，尽管网络安全的技术不断进步、网络安全投入迅速提升，但重大的安全事件仍然时有发生。因此，在网络攻击面前，即使个人消费者与组织用户采取了周密的网络安全防御措施，仍不可轻视网络攻击的巨大威胁。”

#### 以下是 亚信安全 2016 年 7 大预测摘要：



##



## 关于亚信安全

亚信安全是亚信集团“领航产业互联网”版图中的重要业务板块，于 2015 年由亚信科技对全球最大的独立网络安全软件提供商趋势科技中国区业务进行收购重组，专注于产业互联网安全服务领域，是中国领先的云与大数据安全技术、产品、方案和服务供应商。亚信安全在中国北京和南京设有独立研发中心，拥有超过 2000 人的专业安全团队，以“护航产业互联网”为使命，以“云与大数据的安全技术领导者”为战略愿景，亚信安全坚持“产品、服务、运营三位一体”的经营模式，助力客户构建“立体化主动防御体系”，为国家提供网络安全与云产业安全保障，推动实施自主可控战略。更多关于亚信安全公司及最新产品信息，请访问：<http://www.asiainfo-sec.com>