亚信安全 新闻稿

[即时发布]

亚信安全分析近十年信息外泄事件　揭露黑客盗取信息的一般特征

个人身份信息成泄露最多的信息类型　地下黑市价格在不断下降

【亚信安全】-【2015 年 11 月 19 日】美国家得宝 5600 万信用卡信息被盗、“阿什利·麦迪逊”3200 万用户私密信息被公开、国内超过 5000 万条社保信息或遭泄露、网易邮箱过亿用户信息遭泄露……近年来发生的一连串严重信息泄漏事件让人触目惊心，也让企业对于如何防范信息泄露事件有了更深的思考。近期，亚信安全对近十年全球公开披露的信息外泄事件进行了统计与分析，指出个人身份信息是被泄露最多的信息类型，黑客青睐的信息正随着市场需求不断变动。据此，亚信安全建议企业应该更多的思考被泄露信息的特征，藉此建立更有针对性的防御体系。

亚信安全的分析数据显示：虽然每个行业泄露的信息类型都有所不同，但一般来说，个人身份信息（包括姓名、地址、身份证号码、出生日期、电话号码等）是过去十年泄露最多的信息类型。其危险性在于，如果个人身份信息已被外泄，那么用户金融记录被窃取的概率达到 22%，医疗记录被窃取的概率则达到 23%，这些信息可以被黑客用于做很多危险的事情。

亚信安全业务发展总监童宁表示：“信息泄露不仅关乎消费者的隐私保护乃至网银资产安全，还对企业的经济效益与声誉造成了严重的负面影响。当发生信息泄露事件后，企业往往只关注事件的应急处理，而没有仔细地去思考这两个问题：什么信息被黑客窃取了？窃取的信息去了哪里？这两个问题之所以重要，是因为其说明了黑客窃取信息的根本动机，以及企业防御的重点在于什么地方。 “

亚信安全研究显示，个人身份信息在网络犯罪地下市场的价格近来已经显著下降，因为供给超过了需求。平均来说，个人身份信息价格从去年的 25 元降至 2015 年的 6 元，但是还是有许多网络犯罪分子青睐这些信息，并将这些信息用于身份诈骗、申请贷款或信用卡、注册假账号进行垃圾邮件和网络钓鱼攻击，或是出售给营销公司及诈骗集团。此外，信用卡信息

也已经供大于求，这都是因为过去一年信息外泄事件的规模和次数都在不断增长，所以卖家更倾向于通过大规模打包的方式将这些信息二次出售。

总之，网络犯罪地下市场是个复杂和不断变化的生态系统，市场动态会因为市场对不同信息类型需求而迅速改变。一个很典型的例子是 Uber 账号，其最近成为网络黑市中相当受欢迎的商品，因为 Uber 账号可以让黑客或司机通过“刷单”来获得欺诈性收益。

此外，过去十年的数据还揭露了一个结论——无论你的企业拥有什么类型、多大规模的数据，它都面临被网络犯罪分子所窃取的风险。亚信安全建议，如果企业想要降低这种风险，就必须洞悉信息泄露攻击的特征，并采取恰当的方式来确保信息的安全性，这些方式包括：

- **技术性措施：**包括防恶意软件和防钓鱼程序、网页过滤、访问控制、数据防泄漏（DLP）、漏洞管理、应用程序控制、入侵检测、硬件和软件防火墙、硬盘和设备加密。
- **非技术性措施：**安全培训以及定期进行安全宣传都非常有必要。此外，企业用户最好进行定期的渗透测试，以及实战演练，检验企业抵御和响应攻击的能力，并尽快修复测试与演练过程中暴露的问题。

不断肆虐的信息泄露事件已经向企业充分展现了威胁的严重性与紧迫性。对于企业用户来说，尽快行动起来，并根据信息泄露事件的特征针对性的采取上述措施已经刻不容缓，因为这将在很大程度上决定企业能否保护好自己的信息资产。

##

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