AsiaInfo | 亚信安全

# 安全预警

[即时发布]

## 亚信安全发现勒索软件新变种　Word 文档成为导火索

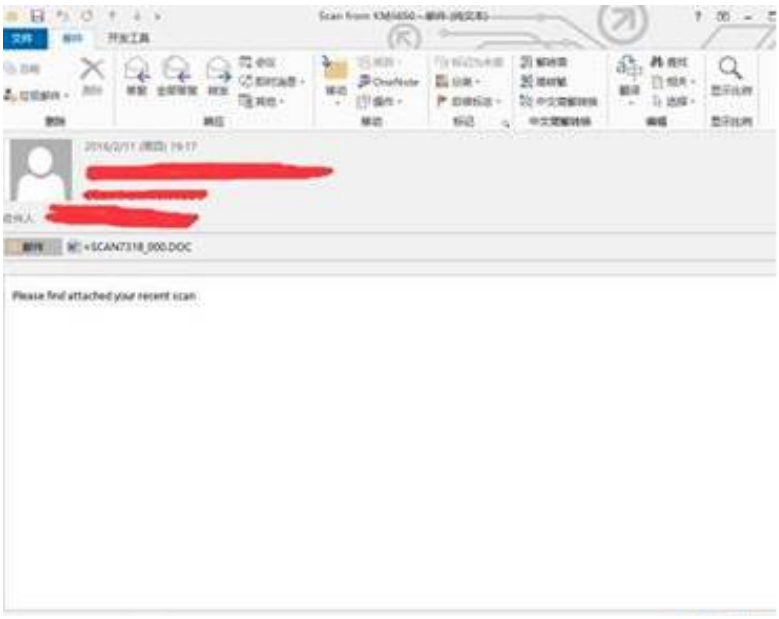
***勒索软件瞄准办公文件　中招可能导致重要文件永远无法解锁***

**【亚信安全】-【2016 年 5 月 13 日】**小心！看到陌生的 Word 文档，你可别急着打开，因为你的重要文件可能因此被非法加密。近日，亚信安全就截获了一个通过 Word 文档传播的 Locky 勒索软件变种，这个名叫“W2KM_LOCKY.B”的勒索软件会随着 Word 文档的打开而自动运行，加密用户电脑中的重要文件，进而勒索巨额赎金。对此，亚信安全建议用户需要格外关注不明邮件、链接、文件，利用安全软件策略封锁勒索软件入侵，或者更新亚信安全产品，有效防范此类勒索软件及其变种攻击。

亚信安全研究人员发现，此次截获的勒索软件变种“W2KM_LOCKY.B”传播方式与之前相似，都是通过伪装成邮件附件进行传播。不同的是，变种病毒的载体不同，之前的勒索软件载体多数为 JS 文件，而此次截获的病毒载体是插入恶意宏代码的 Word 文档。一旦 Word 文档被运行，其会链接特定 C&C 服务器接收和发送信息，并下载勒索软件病毒，继而加密计算机中的 Word、Excle、Ppt 等重要办公文件，还会在桌面上显示勒索信息。


【勒索软件在受害者电脑桌面上显示的勒索信息】

为了感染更多的用户，不法分子很有可能通过社交工程攻击的方式，有针对性地假借邮递服务、电信、公共事业和政府机构通知的名义来制作诱饵，诱使受害者点击并打开邮件中的附件，以获取更多的赎金。




【勒索软件通过邮件来传播】

亚信安全技术总经理蔡昇钦指出：“勒索软件在今年第一季度已经成为用户的头号威胁因素，可能导致用户数据无法恢复乃至钱财被敲诈。而且勒索软件还产生了大量小范围传播的变种，防护难度很大。特别是对于中小企业来说，由于其安全防护能力相对薄弱、支付赎金的意愿较高，因此更容易成为勒索软件的攻击目标。”

**要防范此类勒索软件的攻击，亚信安全建议用户执行以下策略：**

1. 不要打开来自未知或无法验证发件人的电子邮件，当打开邮件附件时，更要注意查看附件扩展名。
2. 不要点击电子邮件中的不明链接，在访问之前可以先检查网站信誉度。
3. 由于许多勒索软件加密的文件暂时无法通过第三方还原，请注意备份重要文档。备份的最佳做法是采取 3-2-1 规则，即至少做三个副本，用两种不同格式保存，并将副本放在异地存储。
4. 亚信安全最新发布的中国区病毒码版本 12.516.60 已包含截止 5 月 10 日收到的所有变种 ,请及时更新病毒码。
5. 使用亚信安全防毒墙网络版(OfficeScan 11 SP1)和 Worry-Free 9.0 SP2 ,开启针对勒索软件( Ransomware ) 的行为阻止策略。


##

## 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