安全小课堂五十八期【勒索软件解析（一）】

京东安全应急响应中心 2017-05-20

点击上方蓝字关注我们！！！

FOLLOW US

全球多家组织遭到了一次严重的勒索软件攻击，西班牙的Telefonica、英国的国民保健署、以及美国的FedEx等组织纷纷中招。发起这一攻击的恶意软件是一种名为“WannaCry”的勒索软件变种,JSRC **安全小课堂第五十八期**，我们来聊一聊勒索软件解析的那些事，本期小课堂邀请到了**球儿**、**齐迹**、**0xgg**师傅进行分享，我感谢JSRC白帽子们的精彩讨论。

简述勒索软件?

京安小妹

通过骚扰、恐吓甚至采用绑架用户文件等方式，使用户数据资产或计算资源无法正常使用，并以此为条件向用户勒索钱财。

讲师： 球儿、齐迹、0xgg

简述勒索软件的原理?

京安小妹

影响用户使用和影响用户的数据。
通过传播途径和攻击方式。

讲师： 球儿、齐迹、0xgg

勒索软件有哪些危害?

京安小妹

锁屏勒索：手机无法使用，类似变砖，你的手机你也用不了。
加密勒索：重要数据被加密，数据丢失，对企业来说，如果重要客户资料、合同、数据库被加密，将直接影响企业正常业务，甚至停产造成极大经济损失。

讲师： 球儿、齐迹、0xgg

勒索软件一般使用什么样的加密方式呢?

京安小妹

对称加密与非对称加密。

AES算法、RSA算法使用最多。

讲师： 球儿、齐迹、0xgg

如果不幸中招应该如何做最大程度减小损失?

京安小妹

第一步:关机、拔网线简单粗暴。
第二步:把硬盘抠出来 在其他电脑上 备份资料。
第三步:寻找有没有可用恢复数据的软件，尝试恢复,如果文件实在没法恢复，又不想支付赎金。那需要彻底格盘以后重装系统,也可以去找专业数据恢复人士进行数据恢复,如果有重要资料，也可以封存硬盘，等后续进展

讲师： 球儿、奇迹、0xgg

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

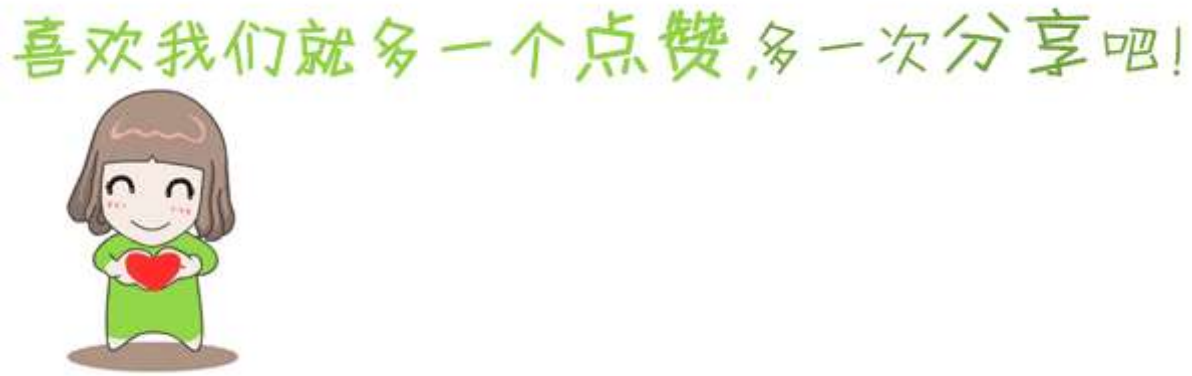
安全小课堂的往期内容开通了自助查询，回复“安全小课堂”或者点击阅读原文进行查看。

最后，广告时间，京东安全招人，安全开发、运营、风控、安全研究等多个职位虚位以待，招聘内容具体信息请扫描二维码了解。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心



阅读原文