安全小课堂五十九期【勒索软件解析（二）】

京东安全应急响应中心 2017-05-27

点击上方蓝字关注我们！！！

FOLLOW US

全球近期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 **安全小课堂第五十九期**，我们继续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。

勒索软件有何特征?

京安小妹

1.行为上，当然是加密文件了。
2.会有弹窗，勒索比特币等虚拟货币。
3.比如发带病毒的邮件，一定会千方百计诱导你下载附件，或者点url下载文件。

讲师： 球儿、齐迹、0xgg

勒索软件的传播途径有哪些?

京安小妹

1.借助网页木马传播，当用户不小心访问恶意网站时，勒索软件会被浏览器自动下载并在后台运行。
2.与其他恶意软件捆绑发布。
3.作为电子邮件附件传播。
4.借助可移动存储介质传播。
5.利用系统漏洞传播。
6.借助xx门传播。
7.bad usb。
8.短信传播。

讲师： 球儿、齐迹、0xgg

针对这些传播途径，如何进行防御?

京安小妹

1. 安装杀毒软件，能防止一部分。
2. 安装补丁,及时更新最新补丁。
3. 保持良好的使用习惯，提高安全意识，下载软件找正规下载网站，下载完进行扫描。
4. 来历不明的电子邮件、附件，不要点击。
5. 很多非法网站，不要去点，容易中病毒,短信啊，聊天过程中人家发的链接啊都得小心。

讲师： 球儿、齐迹、0xgg

企业应该从哪些方面进行保护工作从而避免遭受勒索软件?

京安小妹

1.定期备份重要资料。
2.很多时候企业被攻击是因为存在漏洞，对于漏洞的检测和预防很重要。一旦出现漏洞，应该立即采取相应措施，打补丁或者采取保护措施。
3.建立应用程序白名单。
4.域管控 网络隔离 网段和内外网 。
5.需要加强安全意识培养，前面也提到了，勒索病毒的传播方式有好几种，平时要对内部人员要多做宣传，保持良好的使用习惯，提高安全意识。
6.网络隔离和权限管控是必要的。
7.针对传播途径的预防措施，对企业来说也都是很有用的。
8.可以采购专业的漏洞扫描系统。
9.企业还要有一些应急预案和应急演练,一方面保证不手忙脚乱 一方面通过演练 让员工提高一下安全意识。
10.上硬件也是企业的一个必要措施。
11.还有有能力的话，事件结束之后感染分析也有用。
12.追踪，溯源。

讲师： 球儿、齐迹、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。

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