安全小课堂第七十六期【钓鱼网站攻击与防御】

京东安全应急响应中心 2017-11-03

钓鱼一般是通过电子邮件或即时通信来进行的，它通常引导用户在一个看似与合法网站相同的虚假网站中输入相关敏感信息的细节。大量的事实案例表明，钓鱼攻击给企业造成的损失可以说已经到了非常危险的程度。JSRC **安全小课堂第七十六期**，邀请两位老师分享钓鱼网站攻击与防御,同时感谢白帽子们的精彩讨论。

什么是钓鱼网站攻击?

京安小妹

钓鱼网站通常指伪装成银行及电子商务，窃取用户提交的银行帐号、密码等私密信息的网站。

网站伪造的特点是伪造的页面与真实合法的网站几乎一模一样，无法直接分辨出来，这时候就要仔细看域名信息是否真的合法。网钓者甚至可以利用知名网站自己的脚本漏洞，链接到恶意网站，在不知不觉中获取用户的数据。

讲师： 香山、袁大

钓鱼网站攻击的危害?

京安小妹

窃取账号、窃取个人信息用于贩卖、用于攻击企业网络。
电信诈骗、账号被窃取（游戏账号被盗、财产损失）、公司机密被窃取。

讲师： 香山、袁大

钓鱼网站攻击有哪些常见的技术手段?

京安小妹

电子邮件、即使通讯工具、手机短信、二维码、网页发送虚假广告的方式。
钓鱼网站的话克隆站点、XSS脚本攻击、Oauth。

：

讲师： 香山、袁大

有哪些比较经典的钓鱼网站攻击案例?

京安小妹

希拉里·克林顿总统竞选团队主席John Podesta的电子邮件账号正是这样遭到入侵的。那封电子邮件包含一个指向被专门设计出来的网页的链接，该网页完美复制了谷歌的登录页面。对那些未经训练的人来说，几乎不可能判断出这是一个假冒的网站。你可以再看看用来窃取财务信息和医疗数据的方式与此多么相似。

一个攻击者可能会从一个看起来像是某个官方账号的邮箱给你发送一封看上去很正式的电子邮件，由此开始这次攻击。这封邮件可能会说一些类似"有人试图在其他国家登录你的账号，请更改你的口令"的话。

:

讲师： 香山、衰大

企业如何有效防止员工被钓鱼网站攻击?

京安小妹

1.组织对员工进行网络安全意识的培训，提高员工的网络安全意识。
2.打开网站看清域名。
3.安装安全防护软件。

对于企业内部需要建立一套防御体系：
1.对内建立良好的奖惩机制。
2.建立报告钓鱼事件的机制。
3.注意邮件中的陌生链接，仔细观察域名。
4.邮件网关可以清理邮件中的链接进行排查。

：

讲师： 香山、衰大

白帽子提问：怎么知道别人这么多企业和人的邮箱地址

可以通过信息收集的方式收集到企业的邮箱之后再进行钓鱼。
之前发现有的企业邮箱你提前发一些测试邮件.如果邮箱不对会导致退信,这样就可以列举出有效邮箱了。
也可以通过这个去猜测出公司邮箱的生成规则。

：

讲师： 香山、衰大

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