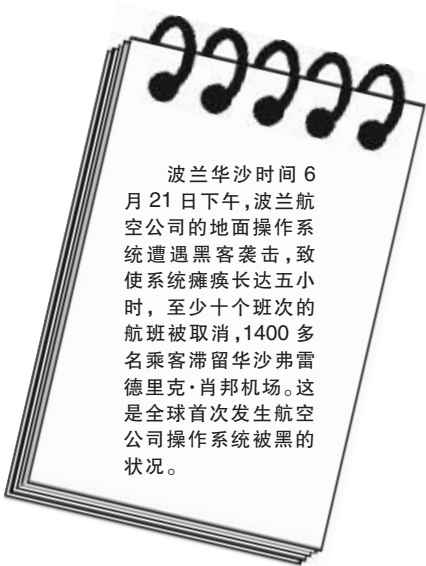


# 波兰民航系统遭黑客入侵

## 航空核心系统首次被黑 波兰安全部门介入调查



波兰华沙时间6月21日下午,波兰航空公司的地面操作系统遭遇黑客袭击,致使系统瘫痪长达五小时,至少十个班次的航班被取消,1400多名乘客滞留华沙弗雷德里克·肖邦机场。这是全球首次发生航空公司操作系统被黑的状况。



波兰首都华沙肖邦机场

## 瘫痪长达五小时

当地时间6月21日16时(北京时间23时),波兰航空公司地面操作系统突然瘫痪,无法建立新的飞行计划,致使预定航班无法出港。

公司方面很快对故障进行排查,迅速判断这是一起黑客攻击事件。

当地时间21时,这家波兰最大的国有航空企业排除了系统故障,恢复了航班。至此,已取消国际航班十个班次,滞留乘客1400多人。航空公司发言人说,乘客安全优先,因此作出取消航班的决定。

经反复确认,这次黑客攻击活动只侵入了地面操作系统中的航班出港系统,并未触及进港系统,因此,所有飞抵肖邦机场的航班并没有受到太大影响。

分析人士称,波航采用全球最尖端的计算机系统,这次黑客事件提醒全球航空业以及同行运营商,黑客技术已经具备入侵航空系统核心部分的能力,应当引起充分重视。波兰安全部门已介入调查。

## 民航网络频繁遭袭

近年来,航空公司接连受到黑客侵扰。今年1月,马来西亚航空公司官网遭黑客攻击,黑客自称隶属于极端组织“伊斯兰国”;同在1月,朝鲜高丽航空公司的“脸谱”主页遭“伊斯兰国”黑客袭击;去年底,美国联合航空公司和美国航空公司网络遭攻击,致使一些常飞乘客的里程数失效。

越来越多的黑客针对航空企业,只是截至波航遭黑前,黑客活动尚未波及航班起降和飞行安全。从黑客的角度来说,攻击民航网站和系统可以为他们自己带来更加深远的影响力,创造一种令人恐惧的效果,但航空专家指出,一旦黑客攻击航空公司核心网络、机场控制系统甚至飞机的飞行控制系统,可能出现比波航系统遭黑更严重的情况,乘客安全可能受到严重威胁。如果黑客受到极端组织的指使,后果将不堪设想。

## 分析

清华大学互联网安全问题专家刘杰博士说,眼下黑客手段越来越高明,黑客技术越来越先进,提高防范意识、及时更新系统、自查系统漏洞等措施不可或缺。

## 端口可能成为漏洞

刘杰说,一般而言,因电脑管理控制系统故障而导致航班大面积延误的情况可能有几种原因所致,要么是系统本身出了故障,要么是人为误操作,再有就是管理控制系统因为漏洞而被入侵。

刘杰介绍,通常来说,机场管理系统或航空公司操作系统软件都是由不同功能的软件模块组成的,这些模块相互之间需要通过端口连接。

设计者在设计软件时通常会预留这些端口,以便日后对某一模块进行更新或开发,而这些人成为端口最易成为黑客攻击的入口。黑客通过扫描可以发现这些端口,并实现破坏的目的。

就在上月,一名美国互联网安全研究者声称自己成功通过美联航的客舱娱乐系统短暂控制了一个航班的飞行系统。

## 建立安全扫描机制

就近期有传言说黑客已经有能力直接进入飞机的飞行控制系统,刘杰说,这种可能性存在,而且随着地空互联的技术推进,可能性越来越大。

因为,现在的民航飞机的操作系统已经不再是一个完全闭合封闭的电脑系统,不再单纯地靠人工无线呼叫建立空地联系或依靠地面雷达的主动扫描获取飞机位置等信息,随着自动化程度越来越高,地空信息联通的通道越来越多,如何管理这些通道和端口成为重

中之重。

刘杰指出,应该尽量减少人为操作失误的可能性,对系统安全进行安全防范意识的加强,减少不必要的互联、避免接入不可信的网络系统。

总之,无论系统多尖端,技术多先进,只要是软件系统,都会留有端口。因此,刘杰建议,公共交通核心系统在日常维护方面应建立定期安全扫描、定期安全检测机制,提高系统整体的防护水平。

(据新华社电)