REAQTA
an IBM Company

IBM

案例研究：
某大型国际机场

在气隙网络中搜寻恶意软件

案例

某大型国际机场通过运行气隙网络，管理从安保到后勤的各种内部运营事务。虽然该机场与外部网络完全隔绝，但仍有一些设备感染了能够在本地捕获和存储信息的恶意软件。

挑战

- 关键基础设施对停机事件无任何容错能力
- 网络内缺乏安全措施
- 气隙网络中同时连接了低安全性和高安全性设备
- 无法清晰了解气隙环境内的任何设备

解决方案

- IBM® Security ReaQta 采用 NanoOS 技术，可清晰洞察各类端点设备和基础设施。
- ReaQta 行为引擎可在孤立网络上运行，而不产生性能降级。
- ReaQta 提供强大的威胁搜寻功能，可重现事件并进行事后分析。

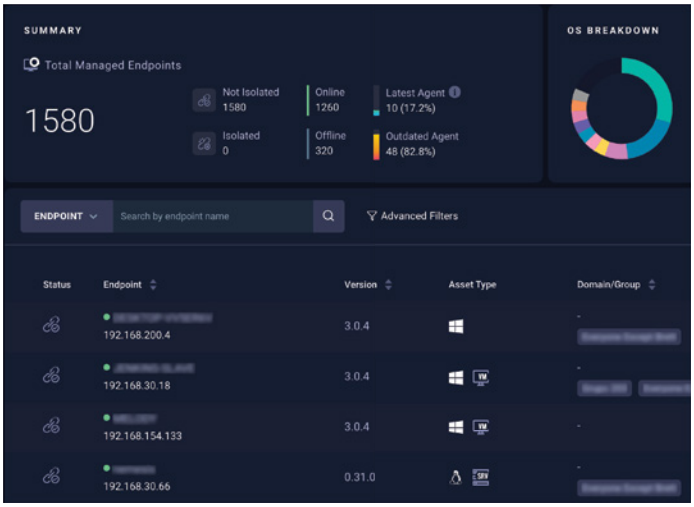
公司

该大型国际机场是世界上最大的交通枢纽之一，每年客运量达 7,000 万人次，每天起降航班超过 1,000 班。该机场被归类为关键基础设施。

安全挑战

总体而言，该机场遵循着出色的安全协议， 采用完全隔离的网络来运营多项关键服务和防止来自互联网的感染。然而，气隙网络创造了一种虚假的安全感。尽管气隙环境内的所有设备都无法访问互联网，但其中的每个网段都相互连接，没有流量控制。

此外，气隙网络包括可供公众现场使用的设备，例如信息亭，这使关键服务面临潜在的攻击威胁。而且，由于将信息从外部带到内部的唯一方法是使用 USB 驱动器，机场员工可在无意中引入潜在的恶意软件，导致端点设备易受攻击。



过程

由于某些端点设备的运行速度存在下降的迹象，该机场聘请 IBM 旗下公司 ReaQta 对其气隙网络进行卫生检查。在初始网段上部署 ReaQta 后，引擎在少数设备上发现了潜在的恶意活动。根据最初的分析，某个可公开访问的信息亭是最初的入口点，但随后的分析发现了第二个入口点：来自值机区的某台设备。这两个恶意载体传播到了涉及不同网段的有限数量的设备。

由于 ReaQta 平台提供的可见性，该机场可在不破坏业务连续性的情况下，重现从初始点开始的事件全过程，并安全地修复感染。

根本原因分析
最初的部署发现了几个行为异常。某个应用程序在内存中安装了键盘记录器，方式是将其注入默认浏览器的隐藏实例中。之后，另一个线程清理了磁盘，以查找 Microsoft Word 文件、PDF 文件、Cookie 和浏览器数据库。这些信息被收集在一个隐藏文件夹中，并且攻击者定期尝试将其发送到某个命令和控制 (C2) 服务器，但由于网络与外界完全隔离而未能成功。

对感染载体的更深入研究揭示了有趣的结果： 该载体异常大，包含一系列旨在绕过本地防病毒软件和沙盒分析的机制。大尺寸很可能是为了逃避防病毒仿真引擎，因为此类系统通常会模拟整个二进制文件的一小部分。

最后确定了两个不同的载体，一个安装在公共信息亭，另一个安装在作为值机管理网络传感器一部分的设备上。尽管这两个载体看起来不同（这主要是因为有大量用于避免检测的垃圾指令），但恶意软件似乎是相同的。两个载体都试图联系同一个 C2 服务器，并以相同的方式运行。

攻击重构
仅在入侵后部署 ReaQta 并不能获得所有信息，并且本地基础设施仅记录最基本的操作系统级别的少量日志。尽管信息量很少，但后续分析显示，感染发生在五个月前，两个端点设备由两个不同的 USB 驱动器感染，时间相隔几天。这两个载体又感染了其他端点设备，而感染原因主要是密码强度较弱，恶意软件尝试在它可以连接的每台设备上随机匹配密码。恶意软件不断收集信息，并且似乎没有采取任何保留控制措施或对其存储器施加限制。恶意软件每八小时便尝试一次与 C2 连接，但由于气隙环境而从未成功。

最终分析表明，虽然该恶意软件具有自我复制能力，并且可以自动将其存储内容复制到外部 USB 驱动器中，但该功能并未启用。据推测，数据外泄过程应该是手动启动的。

响应和补救
ReaQta 的补救模块清理了受感染的设备，并清除了所识别的存储文件夹，以避免任何数据泄漏。实践证明，除了已识别为受感染的设备外，威胁搜寻界面对于确认整个基础设施均已排除相同载体至关重要。ReaQta 进行了行为搜索，以确保在其他设备上检测不到任何恶意软件实例。搜索范围包括所有已识别的行为、持续威胁和数据收集方法，直到可以确认基础设施中不存在该载体及其变体。

最后，本地安全团队建立了一套更严格的内部流量控制规则。网络的公共部分与内部运营相隔离，而且本地安全团队开始运行持续的端点监视和定期的威胁搜寻活动。

结果

气隙环境可以实现极高的安全性，但如果不以严格的方式实施，可能会产生一种虚假的安全感。尽管攻击动机仍不清楚（因为数据虽然被收集，但从未被泄露），但我们可以肯定地断定攻击者撬开了基础设施的大门，因此不仅可以外泄信息，还可以积极破坏机场的运营。对值机区发起简单的勒索软件攻击，就会造成不可避免的延误；而对安检区发起同样的攻击，则会彻底阻止航班并造成严重影响。

如需了解更多信息，请访问：
ibm.com/cn-zh/products/reaqta

国际商业机器(中国)有限公司
北京市朝阳区金和东路 20 号院 3 号楼
正大中心南塔 12 层
邮编:100020

美国出品
2022 年 4 月

本文档为截止最初公布日期的最新版本，IBM 可能随时对其进行更改。IBM 并不一定在开展业务的所有国家或地区提供所有产品或服务。

本文档内的信息“按现状”提供，不附有任何种类（无论明示还是暗示的）保证，包括不附有关于适销性、适用于某种特定用途的任何保证，以及非侵权的任何保证或条件。IBM 产品根据其提供时所依据的协议条款和条件获得保证。

良好安全实践声明： IT 系统安全涉及通过预防和检测来自企业内部和外部的不正当访问并做出相应响应来保护系统和信息。不正当访问可导致信息被更改、破坏、盗用或滥用，也可能导致系统被损坏或滥用（包括用于攻击他人）。任何 IT 系统或产品都不应被视为完全安全，任何一个产品、服务或安全措施都不能完全有效防止不正当使用或访问。IBM 系统、产品和服务旨在成为合法、全面的安全措施的一部分，这必然涉及其他操作程序，可能需要借助其他系统、产品或服务才能发挥最大作用。**IBM 不保证任何系统、产品或服务可免于或使您的企业免于受到任何一方恶意或非法行为的影响。**