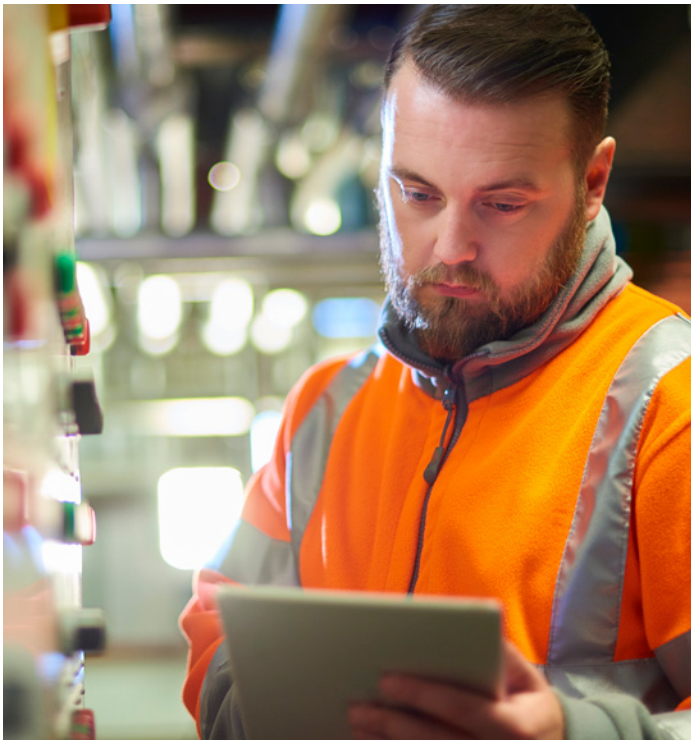
REAQTA
an IBM Company

IBM

案例研究：
关键的基础设施

跟踪一个针对水资源管理机构、高度复杂的供应链攻击



客户案例

一个外来攻击主体通过供应商对水资源管理机构发起攻击。运营商注意到有可疑活动，但认为那只是外部安全服务提供商的维护工作。攻击者设法获得访问权限，并在运营商的网络中横向移动、扩散。攻击者试图泄露该管理机构的内部信息，然后破坏高级服务器，并部署基于勒索软件的反取证措施。

面临的挑战

- 该机构作为负责其运营区域的水资源分配的关键机构，容易受攻击危害
- 不具备检测和搜寻无文件威胁和横向移动的能力
- 缺乏针对勒索软件的保护
- 用于端点安全的资源有限

解决方案

- IBM® Security ReaQta 采用 NanoOS，具备无法检测的特点，确保各端点和基础架构均拥有无可比拟的可见性
- 在本机跟踪横向移动和异常登录尝试
- 提供针对勒索软件攻击的本机保护
- 提供强大的威胁搜寻界面，能跟踪和重建高度复杂的事件

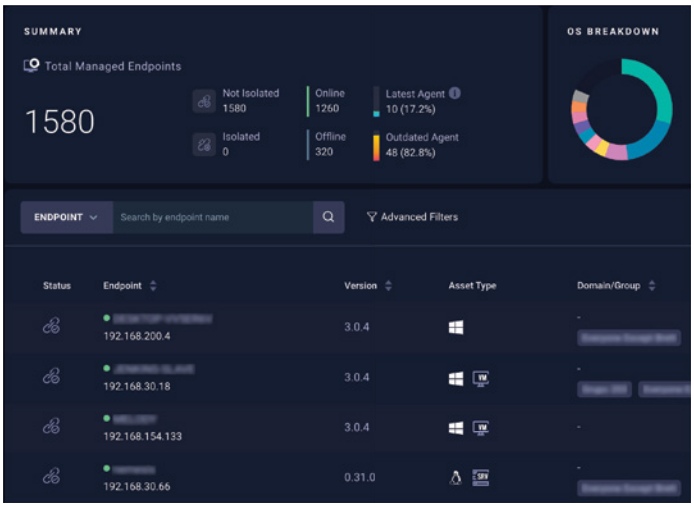
客户简介

这是欧洲的一个水资源管理机构，负责处理和分配大约 100 万人的供水储备。类别上属于关键基础设施和基本服务。

安全性挑战

关键基础设施的站点必须不断应变，以应对日益繁杂的网络风险和越来越多的来自各种威胁主体的复杂攻击。关键基础设施管理着重要的资源，容易成为攻击者的理想目标，受到攻击，造成重大影响，导致高度敏感数据外泄。

该水资源管理机构仅有传统的网络分析工具，但没有端点监控，也没有应对攻击的能力。那些工具无法跟踪跨端点的操作，例如横向移动。此外，该机构普遍缺乏 IT 资源，运营商需聘请外部提供商来管理电子邮件、DNS、VPN 和防火墙等基本服务，因此，在不同提供商之间协调工作变得更加纷乱复杂。



NanoOS 是一种基于虚拟机管理程序的独特方法，可在操作系统外部工作，并为端点上运行的进程和应用程序提供深度可见性。

进程

IBM 旗下 ReaQta 公司受该机构委托，在其所有服务器、台式机和笔记本电脑上运行其解决方案，进行持续监控，并及时跟踪和调查潜在的安全漏洞。ReaQta NanoOS 技术采用内置人工智能双引擎和细致的行为分析，为此基础设施提供全面的可视化管理，确保可对端点进行实时查询，可广泛搜索入侵指标 (IOC) 和行为指标 (IOB)，还可进行高级数据挖掘以发现休眠型威胁。

解决方案部署六个月后，代理商检测到初始异常活动，于是对攻击者访问一组特定数据集的整个过程进行了跟踪。而该机构采用的传统防病毒软件和入侵检测系统 (IDS) 并未检测到任何攻击活动，直到最后阶段才发现。如果没有 ReaQta，攻击者就会成功获取、泄露数据，擦除整个基础架构以掩盖其踪迹。

针对供应链的攻击

在首次攻击发生的当天，ReaQta 就发现了一次从 VPN 服务器到非特权网段里的端点出现的可疑登录，并作为警报予以标记。安全人员认为这次登录只是外部安全提供商的维护工作，因此并未高度重视。攻击者设法部署了第一个恶意软件，主要用于映射网段，寻找通向特权网络的直接路径。但攻击者发现没有这样的路径可用，于是决定在内存中部署第二个恶意软件，用于收集登录凭证，从而在随后的横向移动中重复使用。获得此类凭证后，攻击者继续行动，访问域控制器，然后很快到达包含内部文档的文件服务器。在攻击的最后阶段，攻击者在整个基础架构上部署一个勒索软件，以掩盖自己的踪迹。

根本原因分析

最初的异常登录发生在轮班时间之外，来自通常与服务器（而不是工作站）互动的端点。该 VPN 通道由外部提供商管理，此外该提供商还负责维护邮件服务器和防火墙。由于此访问的性质有异，警报对此保持激活状态，以跟踪每个操作，但此时内部安全团队以为是提供商在对基础架构进行维护，因此没有高度重视。

第二天，ReaQta 发出了第二个警报，显示出现轻量级恶意软件扫描内部网络的活动，随后很快又发出另一个警报，表明内存中存在具有键盘记录和凭证收集功能的向量。攻击者通过一系列横向移动终于访问到了一个域控制器，此时，安全团队开始重视这些事件，启动威胁搜索会话。该团队决定利用 NanoOS 技术的隐蔽性，尽可能长时间地跟踪攻击者，以了解其操作方式及其目标。

当攻击者试图到达包含高度敏感信息的文件服务器时，安全团队决定阻止他们并启动根除计划。安全人员对各种设备采取了补救措施。攻击者发现，尽管他们能进行很高级别的访问，但却无法访问到想要的信息。他们意识到自己被发现了，于是在整个基础架构上部署了勒索软件以掩盖踪迹。

攻击和重建

运营商了解攻击的动机之后，还需对该攻击进行全盘了解，以对其基础架构中的薄弱环节进行加强。受到攻击的设备数量，在部署勒索软件之前（第 1 阶段）有十多个，之后（第 2 阶段）有数千个。

攻击者设法获得了对 VPN 和邮件服务器提供商的访问权限，用作进入内部网络的初始入口。攻击者复用提供商的凭证来移动到多个不同的计算机中，最终在某个特定的工作站上安置下来。这时候，他们使用一系列工具来扫描内部网络，确定横向移动的目标。在最后阶段，他们用域控制器本身把勒索软件传播到每台设备。

响应和补救

对 VPN 访问加以保护，用威胁搜寻会话识别攻击者攻入的每台计算机。ReaQta 补救模块自动执行清理过程，几秒钟内就清理了该片段。侦察和横向移动阶段所用的所有工具都已到位，一项包括 IOC 和行为的策略立即在整个基础架构中部署传播到位。此策略部署后，不再发现有主机受到影响。立即重置所有用户的凭证，此后不需要对勒索软件攻击进一步干预，因为所有设备都启用了 ReaQta 反勒索软件保护，防止重要信息丢失和正常活动中断。

此事件第二天即成功结束，没有任何数据丢失、基本服务中断或端点损坏。

成果

IBM Security ReaQta 悄无声息地跟踪了攻击者的行动，直到安全团队关闭其访问，后来部署了 ReaQta 解决方案来清理受感染的设备，没有引起停机。如果没有 ReaQta，敏感信息肯定会被泄露，攻击者可能会保持活跃很长时间，最终以勒索软件攻击整个基础设施，使之瘫痪。这种毁灭性的攻击可能造成重大影响，使当地必不可少的水资源供应遭到损害，并可能完全停摆。要想识别供应链的攻击，难度很大，如果没有获得取证信息来查明攻击的根本原因，则该机构今后有可能再次遭到来自同一攻击渠道的破坏。

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 5 月