MANDIANT®

解决方案简述

利用 Mandiant 托管防御减缓战略性勒索软件威胁

优势

- **查看最重要的警报**
  请专家监控整个环境中的技术警报，并确定、调查和确定优先级。您可获得范围较小的优先事项，并与背景关联。
- **接触隐藏攻击者**
  通过映射至 MITRE ATT&CK 框架的主动威胁搜寻，可检测隐藏的漏洞和潜在网络攻击。
- **快速中断与响应**
  Managed Defense 专家通过 Mandiant 事件响应人员和安全分析师的集体知识和经验，支持您应对攻击。
- **升级您的团队**
  我们指定的安全专家团队将培训您的团队，为其提供建议并与其合作，传授他们与众不同的网络安全知识，并使您更深入了解此理论或您的环境。
- **升级您的防御**
  通过根据相关威胁情报进行持续评估和建议，增强您的安全态势。

自 2017 年起，勒索软件攻击的频率和严重程度快速增加。在复杂的多阶段攻击中，老练的攻击者采用了最初被认为是令人讨厌的方法，这些攻击将数据加密与数据暴露的威胁相结合。在同一时间内，这些参与者从广泛播种这种恶意软件威胁扩展到针对特定组织和行业（包含整个城市）。如今，勒索软件攻击的总成本可能攀升至数百万美元。

这种演变的威胁促使许多组织评估、开发和更新潜在的反勒索软件策略，以加快其响应速度。Mandiant Managed Defense 等有效托管检测和响应 (MDR) 功能，可以减轻 APT 集团战略性部署的勒索软件等威胁的风险，并向您的高管和董事会保证安全能力已经到位。若要内部实现这些功能，可能需要一定的时间和资源。

Managed Defense 有助于抵御勒索软件

对于面临高级勒索软件战术和威胁的组织，Managed Defense 提供专家支持，以日常响应和预防有动机的对手。

查看在所有威胁矢量中都很重要的威胁

想要使用勒索软件的攻击者可以通过各种威胁媒介（包括远程桌面协议、带有恶意链接或附件的鱼叉式网络钓鱼电子邮件或通过恶意网站的按驱动器下载）进入受害者的环境。入侵后，这些攻击者识别关键系统和数据，以最大限度地提高其任务的成功机会。

对于大多数组织来说，从无数的终端到当今快速扩展的网络外围环境，获得对整个企业的可见性和控制对于检测复杂的攻击后危害至关重要。Managed Defense 并不停在终端，而是保持端到端网络可见性，以识别异常行为，并确定关键调查警报的优先级。此外，Mandiant 专家使用电子邮件活动识别新攻击者趋势和勒索软件交付机制。

识别勒索软件威胁模式

在组织内配备接触过解勒索软件攻击者策略、技术和程序的熟练分析师，比以往任何时候都重要。为了实现他们的目标，战略勒索软件攻击者需要首先建立立足点，然后保持与受害者环境的联系。例如，Mandiant 专家发现 MAZE 威胁参与者在横向通过受害者网络移动后，在许多服务器和工作站上安装了有效负载。然后，该团队能够获取和维护访问权限，升级权限并开始横向移动。

2019 年，Mandiant 发现，对于 APT 威胁组织在事件响应客户中战略性部署的勒索软件，部署勒索软件之前的平均停留时间是 72 天。虽然 APT 威胁组织还针对 Managed Defense 客户进行勒索软件攻击，但在几乎所有情况下，勒索软件组件在部署前都已检测到并缓解。这将客户的战略部署勒索软件平均停留时间从 72 天缩短到 24 小时以下。(图 1)

图 1.

2019 年，Managed Defense 可显著减少客户战略性勒索软件的停机时间

若要检测此类战略勒索软件攻击，组织必须首先发现这些隐藏的攻击者；许多组织未雇用熟练的、掌握当前和以往攻击者行为的专业知识的威胁猎人。Managed Defense 威胁搜寻团队依靠前线网络威胁情报和独特的事件响应经验搜寻战略性勒索软件威胁。

在产生影响前响应

由于勒索软件可以迅速感染和加密，因此快速有效地响应战略勒索软件至关重要。最近发生的勒索软件攻击范围很广，需要安全团队确定攻击者活动的全部范围并彻底解决。Managed Defense 提供全天候监控和警报优先级，因此 Mandiant 专家可以快速确定优先警报的范围和调查。

Managed Defense 利用超过 15 年的高调事件响应经验，提供快速评估和遏制威胁。Managed Defense 顾问与 Mandiant 事件响应专家合作，发现并阻止环境中的攻击者活动。这些快速响应约定可防止客户在 98% 的时间产生完整的事件响应成本。Managed Defense 查找功能根据团队数据合作开发，并通过全面的报告在 Managed Defense 门户中提供。

要详细了解 Mandiant Managed Defense 如何帮助您的组织发现和响应战略勒索软件，请访问 **www.fireeye.com/managed-defense**

FireEye
中国上海市黄浦区淮海路东段淮海中路 99 号大上海时代广场 26 楼
china@fireeye.com

关于 Mandiant Solutions

Mandiant Solutions 将全球领先的威胁情报、一线事件响应数据、持续的安全性验证结合，为组织提供了所需工具，以提高安全性和降低业务风险。

MD-EXT-SB-US-EN-000335-01