SOPHOS
Cybersecurity delivered.

威胁追踪入门

准备搜索和消除难以捉摸的网络威胁的实用指南

网络攻击在不断进化。对手越来越多地转向复杂且高度回避的方法，协助和执行其攻击。因此，追捕并消除恶意活动的做法在对抗此类高级威胁时非常关键 – 但这并不容易。

在本报告中，我们提供威胁追捕入门指南，以及安全团队用于帮助其领先最新网络威胁并快速响应任何潜在攻击的工具和框架总结。我们还将提供 IT 专业人员准备威胁追踪应遵循的 5 个步骤。

2022 年网络威胁现状

攻击数量、复杂程度和影响都增加

企业面临的网络安全挑战继续增长。去年 57% 的企业遇到的网络攻击数量增加，59% 的企业遇到的攻击复杂程度增加，53% 的企业遇到的攻击影响都有所增加。几乎四分之三 (72%) 的受访者认为至少在上述其中一个方面有所增加。

供应链攻击增加是一个不断增长的趋势，例如 2021 年 3 月披露的 SolarWinds 事件。攻击者在用于远程管理复杂网络的 Orion 解决方案源代码中插入修改过的指令。此后门允许对手访问 SolarWinds 客户的网络，包括多个政府机关。

勒索软件是所有企业面临的现实威胁

66% 的企业在去年受到勒索软件攻击，2020 年为 37%。一年内增长了 78%，说明对手明显更加擅长大规模开展攻击。

合法工具在网络攻击中的使用增加

对手越来越多地利用非法买卖或盗版的合法现成软件和免费开源工具。通常此类工具设计用于模拟网络攻击以提高安全性，但罪犯可以用于相反用途。

类似 Mimikatz 的工具（渗透测试人员和恶意软件作者等使用）虽然不是严格意义上的商业产品，但使用广泛，几乎出现在 Sophos 去年调查的所有手动攻击事件中。

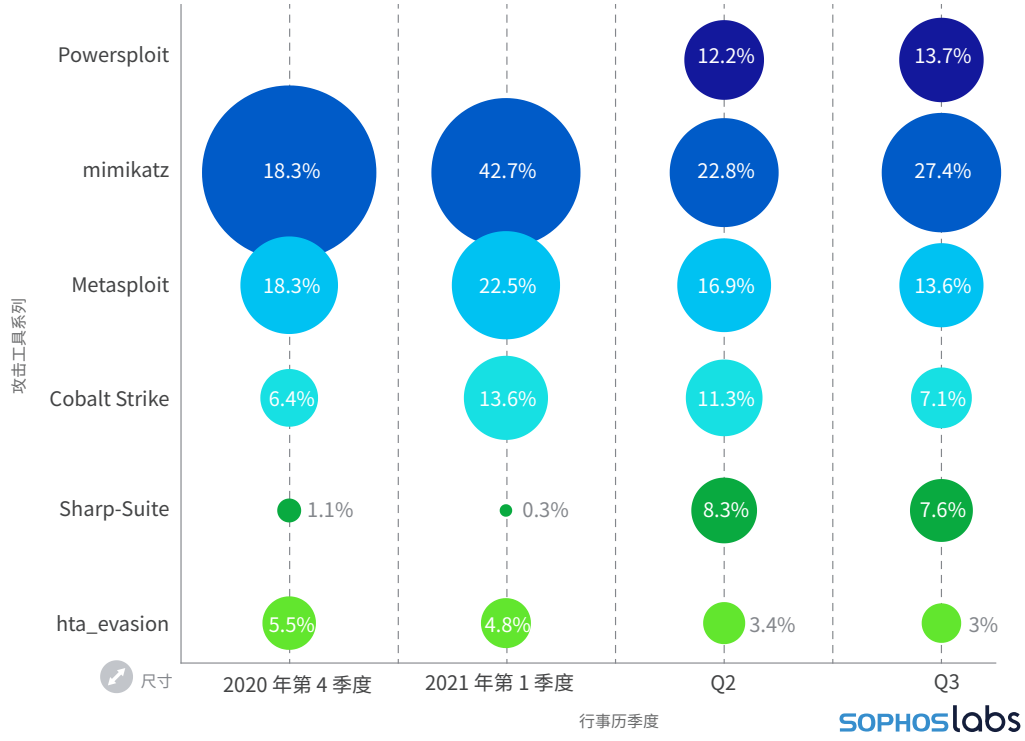
此外，值得注意的是攻击者仿真软件 Cobalt Strike 的盗版副本，由于其源程序码在 2020 年外泄，不仅用于勒索软件攻击，还作为其他恶意软件初始载荷投放。

[1]2022 勒索软件现状 - Sophos

[2]2022 勒索软件现状 - Sophos

主要顶级攻击工具的流行

按计算机数来看，2020-2021 年最经常遇到的攻击工具



Sophos 2022 威胁报告

Cobalt Strike 的“Beacons 信号灯”功能，提供 Windows 计算机后门，意味着软件已经成为网络罪犯喜欢的工具。因此，我们去年见过的大部分勒索软件案例涉及用到 Cobalt Strike 信号灯。

有关目前网络威胁现状的更加详细概述，请查看最新 Sophos 威胁报告。

主动网络安全做法是必要的

供应链攻击。软件漏洞利用。合法工具。共同之处是这些方法的性本质。他们由人主导。他们目标明确，精心计算。他们避开传统手段，无法发现。

企业必须转向更加主动的网络安全做法，以便始终领先罪犯。应对人类对手需要人为主导的方法。

进入威胁追踪。

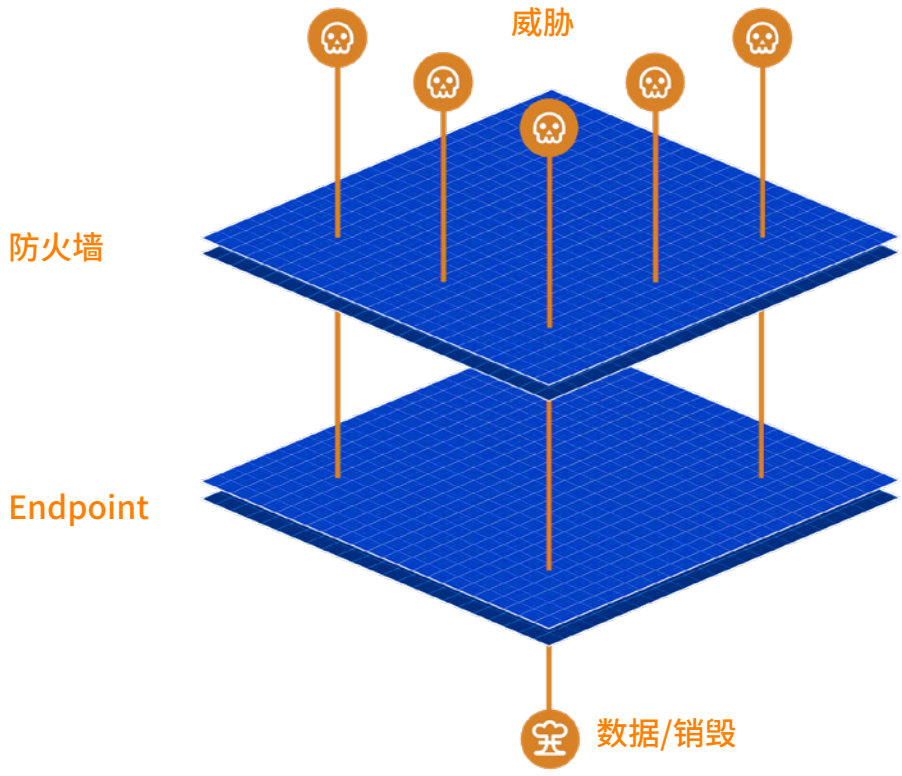
什么是威胁追踪?

威胁追踪是在端点和网络遥测范围内迭代主动搜索以发现恶意活动的过程，假定对手已经避开防御。我们将其标记为迭代是因为此做法需要不断调整适应，确保其一直是搜索并消除现在同样不断发展的网络威胁的有效方法。

在威胁追踪中，团队将分析威胁操作者采用的工具、技术和过程 (TTP)，以确定攻击阶段和构建情报。确定后，他们将采取合适措施消除威胁（如果需要）。

为什么我们需要威胁追踪?

理由有很多，但最重要的理由是一个简单的事实：虽然说法不计其数，但单纯技术无法 100% 阻止威胁。虽然采取多层防御，但一些威胁仍然想办法进入并威胁 IT 资产。



我们已经提到，现代威胁操作者越来越多地转向适应性回避方法，即字面意义的“键盘操作”，而不是去年广泛的自动化攻击。

我们威胁响应团队的发现体现了这一点，他们报告控制并驱动攻击的人类对手数量显著增加。这意味着安全团队必须追踪未知威胁以保持领先，同时调整假设外泄已经发生的思维方式。

威胁追踪心态

经验丰富的威胁猎手通常假定潜在威胁已经避开防御，无论其在攻击链中任何位置。他们采取这一心态可强迫其做两件事。

限制威胁操作者驻留时间

采取此心态迫使团队限制威胁操作者的驻留时间。黑客在您的网络内停留时间越久，执行恶意活动的时间越多。因此，给予对手停留在网络内的时间越短，他们可以造成的破坏越少。安全团队必须假定防御已经被避开，在感受到影响前找出威胁。

缩短侦测时间

采取此心态还可迫使团队缩短平均侦测时间。您可能有多层防御，有躲避能力的威胁可能会沿着在其攻击链进一步触发防御机制。问题在于，此时已经为时过晚 – 破坏已经完成，威胁已经入侵过远。通过追踪威胁，我们能够确定可以后续处理的安全漏洞，最终缩短未来发现相同或类似威胁的时间。

谁进行威胁追踪?

威胁猎手的特质

在了解谁进行威胁追踪前,务必了解威胁猎手的角色。威胁追踪是一个非常复杂的操作。这个领域的人需要掌握一套特定而独特的技能。即,威胁猎手需要的典型特征包括:

- **创造力和好奇** – 寻找威胁类似于大海捞针。威胁猎手可以用数天时间寻找威胁,利用众多方法寻找。
- **网络安全经验** – 威胁追踪是网络安全中最进阶的操作。因此,以前必须具备该领域经验和基础知识。
- **威胁态势知识** – 了解最新威胁趋势是寻找并消除未知威胁时的必备条件。
- **对立性思维** – 像黑客一样思考在对抗现在人为主导攻击很关键。
- **技术编写能力** – 威胁猎手需要在调查过程中记录所有发现。因此,传递此类复杂信息的能力是从追踪得出结论的关键条件。
- **操作系统 (OS) 和联网知识** – 这两个领域的出色工作知识很关键。
- **编写代码/脚本的经验** – 需要帮助威胁猎手生成程序,自动执行任务,解析日志,执行数据分析任务,以协助和推进其调查。

遗憾的是,IT 领域明显短缺具备这套罕见能力组合的人才,54% 的 IT 管理员认为即使有所有这些工具,网络攻击对于他们的 IT 团队来说仍然过于先进,无法独立处理。即,要填补角色,我们普遍发现由两个不同团队中的一个开展威胁追踪。

内部安全运营中心 (SOC)

如果企业选择自行开展威胁追踪,您将发现他们在 SOC 内雇用。SOC 是一个中央内部业务职能,关注监测、侦测、调查和响应网络威胁,同时提升母公司的整体安全状态。他们是企业内负责网络安全事务的专门团队。

第三方安全运营提供商

许多企业越来越多地将安全运营外包给第三方提供商。这可能是因为缺乏内部能力(去年 IT 团队的网络安全工作量增加 69%),缺乏技能,或者偏好由外部专家执行这项关键的 24/7 全天候任务。

托管式侦测与响应 (MDR) 提供商

以全托管服务形式提供的 MDR 为企业提供专门安全分析师团队,24/7/365 全天候追踪潜伏的威胁。事实上,据 ESG Research 表示,51% 受访者利用托管式侦测与响应 (MDR) 服务提供商帮助整合遥测数据用于威胁侦测与响应。

MDR 提供商相比内部纯安全运营计划具有多个优势。其中最显著的优势往往是经验。

Sophos MDR team 有数千小时见证和处理对手攻击的经验。他们还可以从一个企业的攻击学习经验,应用到所有客户。另一个优势是规模:Sophos MDR 团队可以提供三支全球团队带来的 24/7 全天候支持。

托管式安全服务提供商 (MSSP)

MSSP 受雇管理部分或所有企业 IT 安全运营,允许内部团队更多关注日常任务。MSSP 将提供威胁追踪能力,作为托管服务的一部分。这还包括上面详细介绍的 MDR 服务。

威胁追踪执行人员

端点/扩展式侦测与响应 (EDR/XDR)

要使威胁猎手识别和调查潜在恶意活动，他们需要输入和调查工具。进入 EDR 和 XDR。他们允许猎手快速发现可疑侦测，并彻底调查。

顾名思义，EDR 提供来自端点解决方案的输入。相比之下，XDR 整合更广泛 IT 环境的信号，包括防火墙、移动、电子邮件和云安全解决方案。考虑到对手利用每一个攻击机会，监控的讯号网络越广，越能提前发现。

EDR/XDR 解决方案的一个最大实际挑战是噪声：威胁猎手获得的信号非常多，可能难以找出真正需要关注的。所以务必将 EDR/XDR 解决方案与提前阻止更多威胁的强大端点防护相结合，允许防御者关注更少更准确的侦测结果。

解析威胁侦测与响应

威胁追踪是更大型行动 (威胁侦测和响应) 的一部分。Sophos 为追踪采用威胁侦测与响应框架。这包括五个核心部分。

1.预防

具备强大且正确配置的预防技术（例如端点防护解决方案），使攻击者无法渗透您的网络。更重要的是，还减少每天甚至每小时生成的安全提醒数量。要查看的提醒的越少，安全团队可以更好地发现和关注真正重要的信号 - 在此情况下，人为主导的回避对手。

2.收集安全事件、提醒和侦测

数据是驱动威胁追踪和分析的燃料。如果没有正确类型、数量和质量的信号，安全运营团队难以准确识别潜在攻击迹象。没有环境的数据让分析师的对抗决策更加复杂。如果没有与信号相关的有意义的元数据，分析师确定信号恶意还是良性时存在困难。

3.优先处理重要的信号

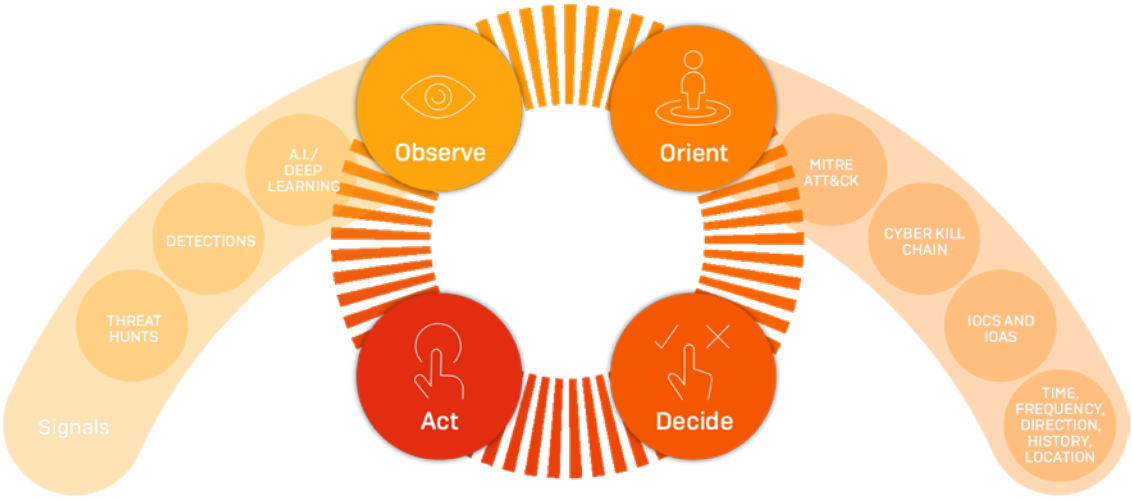
为了避免大量数据淹没，而无法发现确保更贴近调查的信号，您需要能够确定真正重要的提醒。这比看起来更难。利用只有事件生产者可以提供的环境组合以及自动人工智能，才可以改善信噪比。即使自动化也不是一个简单的过程。

4.调查

分离关键信号后，就可以根据行业架构和模型来新增深入信息和评量所得的发现，建立确定恶意或良性行为的信心阈值。

OODA 调查框架

经验丰富的安全分析师通常利用框架指导其调查。例如，Sophos MDR 团队采用称为 OODA 循环的调查方法。这允许他们参与上述循环，确保测试和证明所有发现：



OODA 循环是一个军事概念，让我们的团队进行推理循环，完全理解事件和周围行为。然后他们可以在这些知识基础上，运用人类决策和直觉，确定客户环境内是否存在恶意活动，并根据此信息决定如何应对。

运用 OODA 框架时，Sophos 的安全分析师通常将执行以下步骤：

- **观察 - 我们在此侦测中发现什么？**
  - 与侦测有关的潜在外部和内部连线的观察
  - 确定侦测发生位置，最终用户是否与其相关
- **确定方向 - 我们对此侦测了解什么？**
  - 收集基于证据的数据
  - 了解此攻击或威胁操作者常见或特定的 TTP。用于确定 TTP 的一个此类资源是 MITRE ATT&CK 框架，我们将在报告后面展开介绍。
  - 收集攻击指标 (IOA) 和入侵指标 (IOC) 情报
- **决定 - 此侦测是恶意、可疑还是良性？是否需要采取措施？**
- **行动 – 根据之前的措施，您将怎么做？**
  - **减轻 - 消除 – 重新循环 – 改进。**

5. 操作

这是一个重要步骤。确定正在处理威胁后，您需要进行两件事 – 它们都很重要。

第一是减轻目前问题，第二是记住您可能只是处理攻击的一个症状，还需要追踪并消除根本原因。执行第一件事时不要影响开展第二个工作的能力。

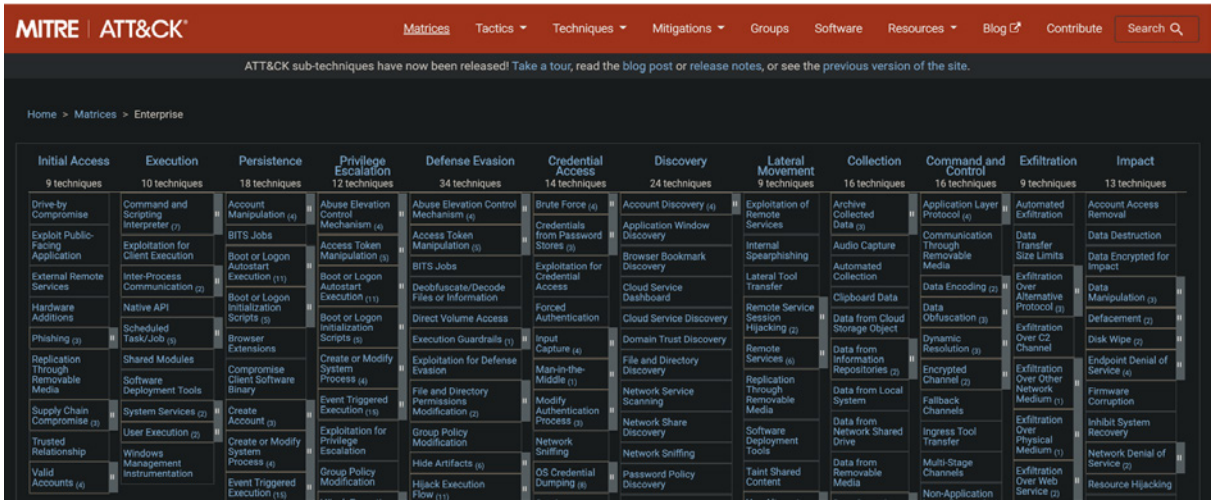
有时候隔离计算机或与网络断开足够了，而有时候安全团队需要深入挖掘网络，找出攻击者的脉络。

例如，仅仅因为您成功阻止并移除系统中的恶意软件，再也看不到相关提醒，并不意味着已经从环境中消除攻击者。

看过数千次攻击的专业威胁猎手知道何时何处更深入挖掘。他们查找攻击者正在、已经或者可能计划在网络中的任何操作 – 并消除这些威胁。

分类威胁：MITRE ATT&CK 框架

MITRE ATT&CK 框架是威胁猎手经常使用的一个资源。如果您在网络安全方面略有研究，很可能至少听说过。在众多框架中，MITRE 是基于现实观察结果的，全球可访问的对手 TTP 知识库，用作建立具体威胁模型和方法的基础。它允许威胁猎手将攻击者对应到多种以前确定的 TTP。反过来允许猎手确定持续攻击所处的生命周期。这对于 OODA 框架的“确定方向”阶段很关键。



您可以在此处了解 MITRE ATT&CK 框架的更多详细信息。

威胁追踪方法

本节将讨论一些常用威胁追踪方法。Sophos 通常以两种不同方式发起追踪。

人为驱动威胁追踪

在我们的组织中，任何需要进一步调查的侦测都交由威胁分析师进行检视，该分析师可以依情况应用业务背景和人类的推理。他们将观察行为，考虑以前确定的业务环境，建立假设，然后采取行动。假设可以主动接合潜在事件，或者进行一些其他调查工作，进一步巩固现有的问题知识。

要完成循环，分析师将等待并查看该假设和测试的结果。如果需要进一步调查，则可以重复此循环直到得出结论。如果事件发展为活跃事件，分析师将专为完全响应模式，主动对抗威胁。

无人引导的威胁追踪

人为驱动追踪需要我们的一个传感器发现或生成感兴趣“信号”，而无人追踪则有机得多。虽然我们仍利用人工智能算法处理我们收集的大量数据，但无人追踪几乎总是由人类威胁分析师掌控。

我们不依赖初始系统信号来提醒我们提供需要调查的地方，而是主动对客户或多个客户的资产进行查询。这样做的原因有多个，包括：

- 同一垂直行业的客户以某种方式成为目标，我们希望尽职调查以确保相同威胁操作者没有尝试攻击我们的任何其他客户
- SophosLabs 已经告知 MDR 团队针对客户的重要攻击，无论是相同垂直行业还是具有类似特性
- 在安全环境中发生重大事件，我们希望确定是否影响到我们的任何客户

案例研究勒索软件捕猎挖出一个历史悠久的银行木马程序

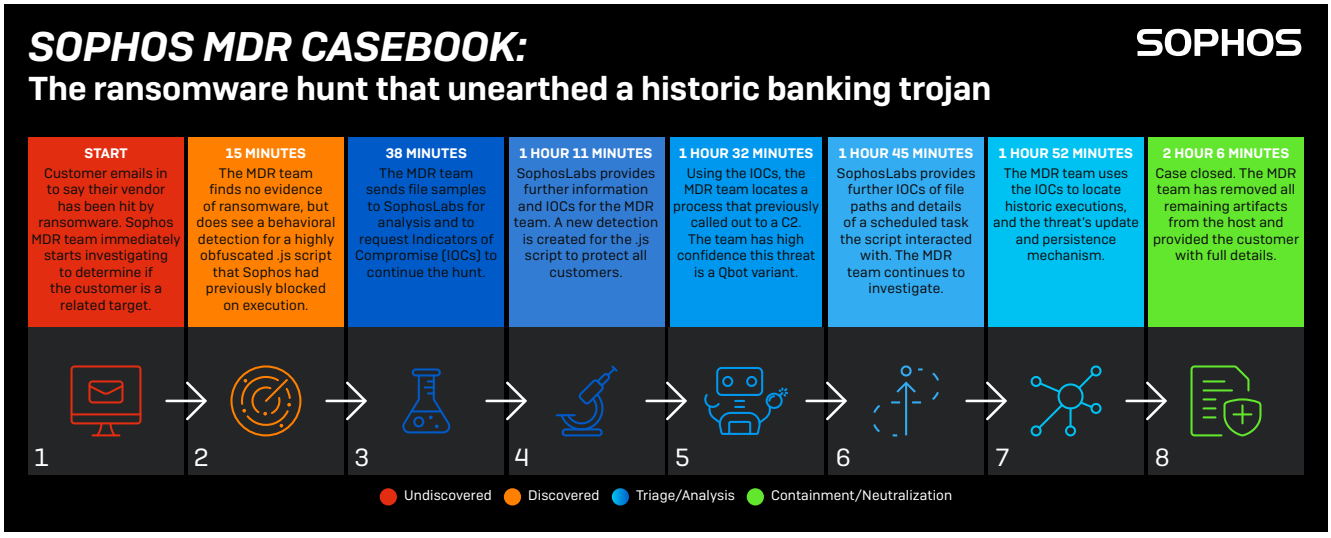
现在我们已经概要介绍了威胁追踪，现在看看威胁追踪实际运作。按照 Sophos MDR 团队的调查，此案例是威胁追踪如何发现意外情况的很好例子。在此案例中，客户联系表示，他们合作的供应商受到勒索软件攻击，他们担心也可能受感染。

Sophos MDR 团队立刻开始调查，与我们的 SophosLabs 专家合作。他们快速意识到没有勒索软件的证据。这时候，有些团队可能结束案件，转向其他工作。但 Sophos MDR 团队继续调查，发现了以前的银行木马。

客户知道自己没有被勒索软件感染，老旧银行恶意软件已经完全移除，可以松一口气 – 如果没有专家接入，这个结果是无法实现的。

正如这个案例所示，虽然勒索软件往往是眼前的威胁，还必须注意往往隐藏在暗处的攻击。

就在 2 小时 6 分钟内，调查并清理整个事件。



要深入了解此案例，请查看此处的文章。

准备威胁追踪 – 支持成功结果的 5 个步骤

现在您应已经很好掌握了威胁追踪的所有相关内容。但开始前，务必确保您的企业具备有效执行的一切内容。

1.了解您当前网络安全操作的成熟度

可以开始了解潜在对手前，您需要了解当前网络安全操作的现状。将进程对应到网络安全成熟度模型（例如 CMMC）是确定开始威胁追踪准备程度（与否）的好方法。审计您的安全状态以确定威胁的敏感程度也是一个好办法。

2.确定希望如何开展威胁追踪

确定网络成熟度后，您可以确定威胁追踪内部进行，完全外包，还是二者组合进行。

3.识别技术差距

检查现有工具，确定开展有效威胁追踪需要的其他内容。预防技术的有效性如何?是否具备或支持 EDR/XDR 带来的威胁追踪功能?

4.识别技术差距

威胁追踪很复杂，需要专业技能。如果您没有内部经验，学习培训课程以帮助培养所需技能。此外，考虑与第三方提供商合作补充您的团队。

5.制定并实施事件响应计划

开始威胁追踪前，务必准备充分事件响应计划，确保衡量并控制任何响应。制定充分准备、理解到位的响应计划，让所有关键方能够立刻采取行动，将极大减少攻击对企业造成的影响。

好的事件响应计划应概述准备、侦测和报告、调查和分析、隔离和消除以及事件后活动的方案。有关制定有效事件响应计划的提示，请参考事件响应指南。

有关准备和开展威胁追踪的更多实用指南，请务必查看 Sophos Threat Hunting Academy。

Sophos 如何帮助

我们已经提到，有效威胁追踪极为复杂，需要下一代技术配合丰富的人为经验。幸运的是，无论您的网络安全成熟度如何，Sophos 都可以支持您的威胁追踪目标。

阻止威胁入侵您的网络 – Sophos Intercept X Endpoint

威胁猎手只要不为安全提醒应接不暇，才能高效开展自己的工作。一种实现方式是引入同类最佳预防技术，这样防御者可以关注更少更准确的侦测，简化接下来的调查和响应流程。进入 Sophos Intercept X Endpoint。

Sophos Intercept X 是行业领先的端点安全解决方案，减少攻击面并阻止攻击运行。结合防漏洞利用攻击、防勒索软件、深度学习人工智能和控制技术，阻止威胁影响您的系统。Intercept X 采用全面深度防御方法保护端点，而不是依赖某一项主要安全技术。

Sophos Intercept X 端点防护的防御功能阻止 99.98% 的威胁（2021 年 1 月-11 月的 AV-TEST 平均分）。然后防御者可以更好地聚焦需要人为干预的可疑信号。

此处您可以更多了解或试用 Intercept X Endpoint。

自己开展威胁追踪– Sophos XDR

Sophos XDR 为专门 SOC 团队工作的安全分析师和负责安全及其他 IT 职责的 IT 管理员设计，支持您的团队侦测、调查和响应端点、服务器、防火墙、云工作负荷、电子邮件、移动等的事件。

从预先编写的、可自定义的、覆盖多个不同威胁追踪与 IT 运营场景的模板选择，或者编写自己的模板，立刻获取对您最重要的信息。您可以访问实时设备数据，长达 90 天磁盘数据，Sophos Data Lake 云存储库中存储的 30 天数据，以及自动生成的可疑项列表，这样您准确了解开始的位置。

如果您要试用 Sophos XDR 开始自己的威胁追踪，Sophos 提供高级威胁追踪和安全运行卫生所需的工具。您可以开始产品试用（如果有 Sophos Central 帐户）或试用 Sophos Intercept X，包含 XDR）。

威胁追踪作为全托管服务或补充您的团队 – Sophos MDR

Sopho MDR 是多方面综合获奖的 MDR 解决方案，为您的网络和云环境带来 Sophos 安全分析师团队的专业技术和技能，以及丰富的能力。Sophos 已经成为您的安全运营的延伸，将丰富的功能带给您。

Sophos MDR 威胁猎手和响应专家团队将：

- 主动搜捕和验证潜在威胁与事件
- 利用所有可用信息确定威胁范围和严重程度
- 对有效威胁布置合适的业务环境
- 采取操作远程中断、隔离和清除威胁
- 提供解决反复出现事件根本原因的可行建议

即使您的企业具有成熟的安全运营中心，您也可能希望额外一双眼睛监测环境，确保不出现任何问题。Sophos MDR 汇聚威胁追踪和端点防护，同时每天提供监管和专业技术。您的网络和云资产是 Sophos 网络分析师和威胁猎手的主要优先事务，他们代表您监测并主动修复和消除威胁。

有了妥当的 MDR 服务，您和您的企业可以安心睡眠，由熟练专家团队持续监测您的企业，追踪威胁，调查可疑活动，响应潜在事件。随着网络安全威胁的不断扩大，与完全关注网络安全的团队合作令人放心。

要讨论 Sophos MDR 如何支持您的企业，请联系 Sophos 代表或申请回电。同时，查看最新 MDR 研究和案例簿。

中国（大陆地区）销售咨询
电子邮件：salescn@sophos.com

22-08-08 WP-ZHCN (PC)