DTA

A collection of 4 posts

DTA

用DTA照亮DNS威胁分析之路 (3)

--- 内置未知威胁分析模型介绍 概述 在系列文章2，介绍了如何利用DTA进行一轮完整的未知威胁分析，共有3个步骤： 1、提出分析思路，从DNS日志里找到可疑线索 2、确认可疑线索有威胁行为 3、借助DNS日志确认资产被感染 其中，这几个步骤里最为安全分析人员所熟悉的应该是步骤2，毕竟日常工作大家都少不了利用各家威胁情报平台、搜索引擎和云沙箱进行信息搜集+关联+确认可疑线索；而步骤1和3，因为涉及到DNS日志，对于不熟悉DNS的分析人员来说，是需要一定学习成本去积累相关分析经验和熟悉DTA的各类元数据的。 因此，针对未知威胁分析，DTA预置了可疑心跳域名、可疑NOD(新出现在网络中的可疑域名)、可疑境外域名等等模型，这些模型以后台运行的方式自动完成上述3个步骤，当模型计算出某个域名存在威胁行为时，会在首页以威胁告警的方式通知分析人员有“未知威胁”类型的告警需要进一步分析。 此时，未知威胁分析的难度和工作强度，降低到了和已知威胁分析差不太多的高度。分析人员只要按照已知威胁分析的模式开展工作，即可完成告警的处置，清除网络存在的未知威胁隐患。 模型 不难想象

· Feb 24, 2022 · 10 min read

DTA

用DTA照亮DNS威胁分析之路 (2)

--- 对服务器网段进行未知威胁分析 概述 要进行网络威胁狩猎，或者低调点叫网络威胁分析，通常需要具备3个能力： 1、找到线索的能力。这里的能力是特指在无先验知识(IoC等)条件下，既尽可能无漏报又不会有太多误报地从海量数据里挖掘出线索； 2、确认线索是威胁的能力。线索是包含噪音的，需要去除噪音只留下有威胁

的线索； 3、分辨资产被真实感染的能力。只有确认真实感染，才能保证后续的威胁处置动作有成果。 按：由于DTA也实现有“已知”威胁分析功能，但其用法和本文描述的操作细节相差甚远，为避免混淆，特此说明一下本文所有威胁分析的用词，都是指“未知”威胁分析。 在上一篇文章，我们提到DNS日志的优点是简单且重要。但正是福兮祸所倚，简单这个优点，从威胁分析的角度来讲它又成了最大的缺点，因为这意味着日志包含的有效信息少。具体来讲，一次DNS请求和回应所解析出来的内容，除去极个别喜欢炫技的特意使用有区分度的词语，比如hackerinvasion[.]f3322.net， hackattacks[.]org等， 大多数日志很难从字面意义上获取有效威胁信息。与此相反，倒是有不少看

· Jan 11, 2022 · 13 min read

DTA

用DTA照亮DNS威胁分析之路 (1)

--- “历史重现”小功能 概述 2021年10月，《七年一剑，360 DNS威胁分析平台》宣告了360 DNS威胁分析平台(简称DTA)的诞生。在文章开头，Netlab阐述了设计DTA的核心理念： 让情报发挥应有价值 让威胁分析真正有效 理念是简洁的，也是抽象的。18个字背后，对应着Neltab 7年的安全研究经验；而7年的沉淀，又在2年时间的打磨里，变成了DTA众多的功能。为了让抽象的理念具象化，后续，我们将推出一系列DTA相关博文，希望通过这些文章案例，在介绍产品某个具体功能如何使用的同时，顺带说明理念是怎样指导功能设计的；也希望这些示例，能为DTA的进阶使用者提供入门参考。 需要提醒使用者的是，DTA是一款灵活的数据分析产品，它一端连接着用户网络的全量DNS数据，另一端连接着360海量云端数据，DTA将这两者汇合，并在平台上努力提供得心应手的各种预置操作工具和大量预处理模型。但全量和海量的二者碰撞，究竟能演绎出多少精彩的内容，绝对是和使用者有极大关系的。在平台上，已经准备好了组件和工具，也有我们一直在更新迭代搭建完成的模型，但模型如何使用，不同的模型如何

· Dec 27, 2021 · 9 min read

DTA

七年一剑，360 DNS威胁分析平台

360Netlab (360 网络安全研究院) 自2014年成立以来，大网安全分析相关技术一直是我们的核心研究方向，我们是最早在国内提出从数据维度做安全的团队 ，并将大数据技术、AI技术和威胁情报应用于大网安全研究工...

· Oct 21, 2021 · 12 min read