DTA

用DTA照亮DNS威胁分析之路 (1)

suqitian
Dec 27, 2021 • 9 min read

--- “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，不同的模型如何组合和拼接，有各种可能性。管理员按照自己的技术能力水平，既可以傻瓜式使用系统内置的数据结果，也可以组合和使用不同的模块及产出

的数据，对DNS的数据进行观察，对用户、告警进行深入高阶分析，请发挥想象，不要被博文介绍的入门内容限制住了思路。

本文是系列文章的第一篇，我们从一个非常简单，即使是新手上路的同学也很容易理解的“历史重现”功能，简单的串下DTA的一些功能元素。

场景

作为公司的安全运营人员，在获取到新的威胁情报时，除了将IoC加入到安全产品，应该还会有这样的疑虑，举例来说：

比如360的安全运营人员，在2021-11-10，当看到ESET在twitter上发布了一则关于Lazarus使用带后门IDA攻击安全分析人员的消息时，他心里应该会想：我们是安全公司，IDA使用普遍，公司内会不会有人碰巧违规使用了这些软件？如果有，是什么时间什么资产在使用？

DTA解决这个问题的理念是：“让情报发挥应有价值”。情报的价值，不应局限于“现在”和“将来”的IoC匹配告警；当新情报出现时，也应该能够在“过去”的历史数据里挖掘出应有价值。

那产品的功能是如何实现的呢？

数据

首先，这个和DTA分析对象有关，它分析的是全量DNS日志数据。

DNS简单且重要。据统计，DNS在企业网全流量里占比小，但超过80%的恶意软件却和DNS协议相关。因此，DTA只要把好DNS这个关口，也能帮助企业发现大部分威胁。具体到真实的公司环境，比如一个拥有6000名员工的公司，日常的DNS流量在10~15Mbps之间，换算成每秒请求数(query per second)，为5千~8千qps，一天的总量大概在7亿。和全流量比，这个量级可以让DTA *以年为单位* 存储全量DNS日志(下文称DNS日志数据库)，而对存储和算力的要求，普通服务器就可以满足。

其次，DTA内部集成了一个mini PDNS，其功能类似于Netlab从2014年开始运维的中国最大公开PDNS数据库(passivedns.cn)，会以极低的成本存储自DTA接入以来

的全量DNS数据，并提供快速查询。

有了这两个数据的支持，在平台上实现“历史重现”的功能就是水到渠成的事情了。

功能

根据IoC数量的不同，DTA平台提供了两种查询方式。还是以ESET提到的带后门IDA例子为例。

单个IoC

在推文里，提供了一个C2域名：devguardmap[.]org。

我们在“全局搜索栏”里选择搜索类别：域名，然后输入或ctrl+v粘贴想要查询的域名，如果该域名在历史上没有被公司内的任何资产访问过，会提示“没有数据”。此刻，您可以放宽心了。

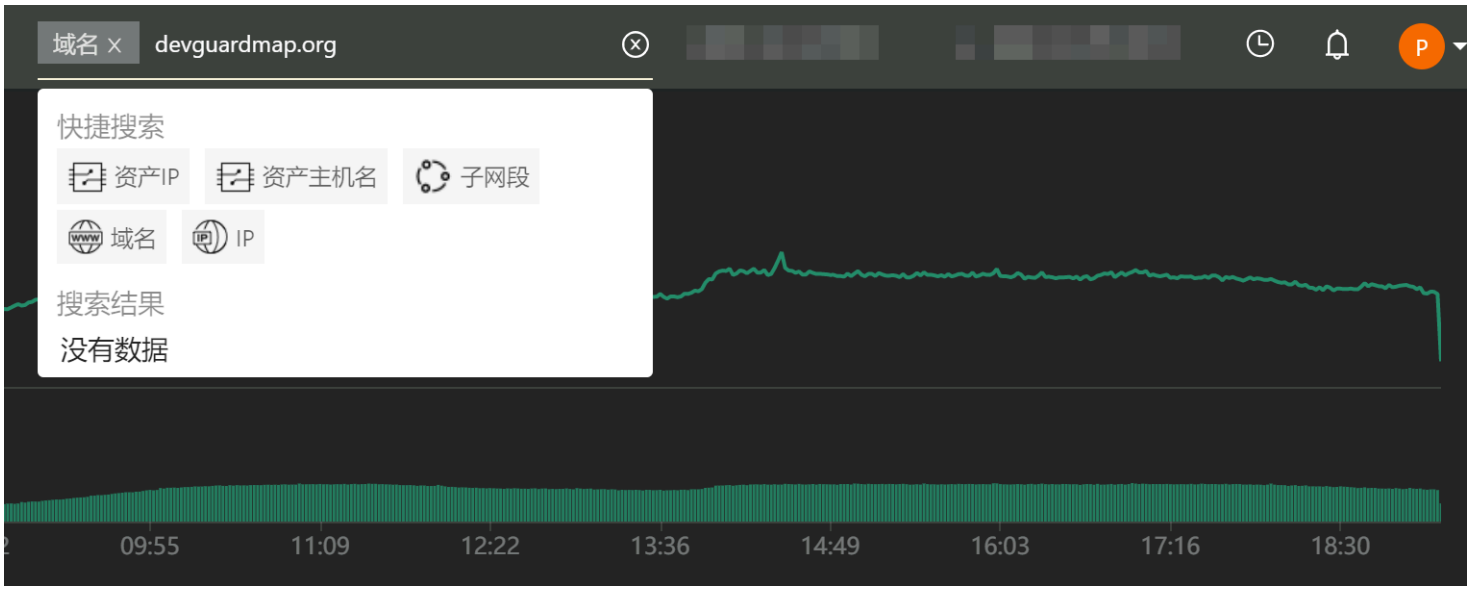

图-1 全局搜索栏无命中

如果有命中，也先别惊慌，进一步选择域名查看详情再做结论。打个岔，从“搜索结果”可以看出，搜索结果会把满足子串匹配的所有域名也都列举出来供选择。

图-2 全局搜索栏有命中

图-3是360内部对该域名的访问情况，两个关键信息：1、在右上角指定的时间范围内，共有11个资产访问了该域名；2、该域名在公司网络内出现的首次时间是：2021-11-11 10:39:25。由于时间是在推文发布(2021-11-10)之后，可以猜测大概率是研究人员在复盘，不是真实的感染。王婆卖瓜一下，360对安全事件的反应还是挺迅速的:)。进一步的，可以点击左侧栏的资产列表，对安全运营人员来说，结合其它信息，能定位到是哪些员工在跟进这个事件。

图-3 域名详情页面

对安全敏感的读者，也许已经注意到域名的下方，有多个tabs，这些tabs里面有DTA系统的多种模型，从数据维度提炼和展现相关对象的多种角度的数据结果，比如这里面有3个橙色的标签：“可疑境外域名”、“UnknownThreat.persistent_access”和“可疑心跳域名”，这些标签是DTA内置的未知威胁模型在分析关联多个维度数据后给出的“可疑域名”判定。橙色标签就像交通灯亮起了黄灯，警示分析人员需要做进一步的分析。至于如何做进一步的分析，找出真实的威胁，后面其它文章细聊。

读者请注意，我们这里举的是一个历史数据的简单匹配，但DTA对这个简单例子的处理方式，和传统意义上的安全事件告警响应系统或者日志查询有很多的不同，如果仔细体会例子的各种细节，应该能感觉到系统从底层数据到页面布局，都是为方便展开威胁分析而设计的。把页面比作操作台，那操作台上既有原材料(用户的DNS数据和360的云端数据)，也有DTA自动产出的大量的预处理结果和不同的各种相关

组件内容(可疑域名标签，资产类别，用户行为偏好等)，类似于乐高片，分析人员按照自己的经验想法，依次组合这些组件，可能就形成了一类有效的威胁分析。依照自己的能力水平，既可以浅尝辄止，也可以持续深入，从完全未知一步步向真相迈进。

多个IoC

在推文里，还出现了另一个域名：www[.]devguardmap[.]org。对多个IoC，DTA通过“威胁分析”页面实现历史数据查询。

“威胁分析”页面提供两种查询方式：1、熟悉语法的，直接书写“查询表达式”；2、不熟悉语法的，在右侧“构建表达式”里分别点击选择查询类别，运算符，输入或选择查询内容，最后点击“应用”按钮开始查询。

查询完成后，通过点击图-4的“2个域名”，“解析到1个IP”，“涉及11个资产”，“共14个请求”等按钮，查询结果会以4种不同的视角，即域名，Rdata，资产，请求时序的角度展现历史DNS请求解析情况。通过更多的角度观察同一份数据，能有效帮助分析人员形成威胁判研。

图-4 威胁分析页面

结语

本文以“历史重现”小功能为起点，通过实例细节，展示了这个功能点是如何和核心理念的第1条对应起来的。您在使用DTA时，也可以多观察，还有哪些功能点是和理念第1条相关的。后面，我们也会继续举例说明。

但下一篇，我们先来谈一谈核心理念的第2条：“让威胁分析真正有效”，看一看DTA是如何将360云端安全数据赋能到用户数据之上的，敬请期待。

产品、商务咨询，请联系 xuyinghan@360.cn

— 360 Netlab Blog - Network Security Research Lab at 360 —

DTA

用DTA照亮DNS威胁分析之路 (3)

用DTA照亮DNS威胁分析之路 (2)

七年一剑，360 DNS威胁分析平台

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...

Log4j

Day 10: where we are with log4j from honeypot's perspective

Our team spent great deal of effort on simulating different protocols, applications and vulnerabilities with our honeypot (Anglerfish and Apacket) system. When big event happens, we are always curious what we see from the honeypot side. Since log4j came to light 10 days ago, we have published two related blogs,

See all 3 posts →

· Jan 11, 2022 · 13 min read

· Dec 21, 2021 · 3 min read