DTA

用DTA照亮DNS威胁分析之路 (3)

suqitian
Feb 24, 2022 • 10 min read

--- 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。

图-1 首页_未知威胁

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，未知威胁分析模型对刚刚接触DTA的分析人员来说，乍听起来会觉得专业生僻，令人心生抗拒。不过如果把模型映射到现实生活，读者把自己代入成朝阳群众那样去分析身边隐秘的线索，会发现模型的原理其实是简单易懂的。首先，按下表做一个映射。

实体	元素1	元素2	元素3	日志的含义
DTA	资产	时间	域名及其Rdata	某资产在某时间请求解析某域名
现实世界	人	时间	地点	某人在某时间出现在某地点

那么，DTA记录在数据库的DNS日志，就如同现实世界里的摄像头，忠实地记录着监控范围内发生的事件。通过分析监控，可以总结出一些可疑情景和模型相对应：

1、某段时间，某人总是在每天的某个时间点准时在某个地方出现。这个情景对应到DTA，属于“*可疑心跳域名*”：就是资产有周期性域名请求，每隔一个固定时间段会发出对该域名的解析请求。DTA部署实践发现，winnit、双枪等多个恶意家族的C2域名在DNS日志上有明显的心跳周期行为。

2、某天，在某个地方出现了一个大家都没见过的陌生人。这个情景对应到DTA，叫做“*可疑NOD*”：即有资产请求了新观测到的域名(New Observe Domain)，这个

域名在以往的访问历史里，从来没有在该网络出现过。可疑NOD适用范围较广，在攻击行为发生的下载、通信阶段等都有机会捕获到线索。

3、如果有某人，经常前往境外的某个地点，这个地点，普罗大众几乎没有前往的记录。这个情景对应到DTA，则是“*可疑境外域名*”：资产访问了一个很少有人请求的境外域名，很少有人请求这个指标是通过统计大网的PDNS数据来度量的，比如自域名出现以来，全中国访问该域名的人数不超过20个。想挖掘高级威胁的分析人员，可以多关注此模型提供的线索。我们曾经测试回溯360发布的APT报告域名类IoC，发现部署在公司内部的DTA，在安全人员利用沙箱测试样本的时候，此模型都能捕获到线索(系列文章1的图-3算是一个不完全恰当的例子--IoC不是360报告)。不过也要保持清醒，找到线索在一个完整的高级威胁分析周期里，大概只能算万里长征的第一里，方向有了，但更多的艰苦在后头。

4、某同事每天上班，总是来回背着鼓鼓囊囊的背包，而其他同事多是两袖清风地上下班，这个情景对应到DTA，叫“*可疑DNS隧道*”：正常的域名请求，前缀相对固定且字符较少，如果某个域名的前缀变化多端，有可能是恶意程序在和C2通信，将偷窃的数据隐藏在正常的DNS请求和响应中。

原理是简单的，难点在大数据的环境下，符合规则的数据量会远超人力可处理范围。以NOD为例，在一个稍有规模（比如1000个员工）的公司网络里，工作日观察到的NOD域名数量可达百万级别，而在休息日，也有十万级别。在这里，借助360云端大数据和积累的经验规则，可以让模型把可疑线索的数据量在尽可能不漏报的情况下降到百或千的级别，然后以可控地方式进入到步骤2和3。

在步骤3，有一个非常值得一提的“自动分析”功能，当该功能分析出告警事件为“无威胁”时，会在告警状态栏打上“无恶意行为”的徽章并给出判断理由。

图-2 自动分析完成_无威胁

除了未知威胁相关的模型，DTA也集成有很多其它类别的模型用来辅助威胁分析。比如可以帮助分析人员判断资产性质的模型，这些模型能标定资产是客户端或服务

器，以及操作系统是Windows或安卓等等；又比如在域名分析页面，为帮助分析人员串起一个事件的前后域名访问关系，集成有共同访问模型。如此等等，不一而足。

举例

前面的原理介绍，说明了模型的思路和使用场景。这一节，我们来个例子介绍一下在DTA是如何处置未知威胁类型告警的。

点击顶部菜单栏进入“威胁告警”页面。页面的第一栏是告警汇总栏，其中，威胁类型分为3类：1、已知威胁和AI识别威胁是由引擎实时匹配IoC产生的；2、网络异常是DNS流量相关的异常；3、本文所描述的未知威胁。

图-3 威胁告警页面_汇总栏

点选“威胁类型”里的未知威胁，页面的第二栏告警列表栏会把指定时间段内的未知威胁过滤出来，通过标题，即可以分辨告警是由可疑心跳还是NOD还是DNS隧道引起的。

图-4 威胁告警页面_告警列表栏

打开状态为“待分析”的事件，进入告警详情页面。页面第一栏IoCs列出域名的基本信息和模型在第2步运行时关联到的判黑情报；第二栏列出当前受影响的资产及其请求恶意域名的概况；在处理完成后，可以在第三栏写下分析经验，供其他人参考。

图-5 告警详情页面

如果想进一步看模型在第2步时的关联关系，点击右上角的“威胁情报图”。

图-6 威胁情报图

根据告警详情页面提供的威胁情报，有逆向能力的分析人员，可以分析样本的行为进一步实锤确认；想轻松一点的可以先尝试通过搜索引擎和各家威胁情报平台搜索关键字，看看有没有相关的分析报告。这个例子里，通过搜索引擎搜索“macapproduct[.]com macos”关键字，可以搜到相关的分析报告，比如《利用EXE文件攻击MacOS》。

至此，仅通过点击查看告警提供的内容和借助搜索引擎，分析人员就可以形成结论：这是一台操作系统为MacOS的资产，被利用exe文件的攻击方法感染了。至于后期的处置动作，因为DTA是被动监听型，必须和其它安全产品配合才能完成清除阻断。

结语

内置的自动化分析模型可以解决普适性的问题并降低安全运维难度和强度。但再丰富的规则也只能描述有限的场景，而网络安全对抗，新手法总是层出不穷，所谓魔高一尺道高一丈。

人的思想是最灵动的，发挥人的能动作用，在未知威胁模型的第1步输出结果上进行深层次的挖掘，有时会有意外收获。下篇举一例子说明如何基于未知威胁最原始的输出上进行威胁分析，敬请期待。

产品、商务咨询，请联系 xuyinghan@360.cn

0 Comments

Login ▾

G

Start the discussion…

LOG IN WITH

OR SIGN UP WITH DISQUS

Name

Share

Best Newest Oldest

Be the first to comment.

Subscribe Privacy Do Not Sell My Data

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

DTA

用DTA照亮DNS威胁分析之路 (2)

用DTA照亮DNS威胁分析之路 (1)

七年一剑，360 DNS威胁分析平台

See all 3 posts →

Botnet

我们近期看到的针对乌克兰和俄罗斯的DDoS攻击细节

在360Netlab（netlab.360.com），我们持续的通过我们的 BotMon 系统跟踪全球范围内的僵尸网络。特别的，对于DDoS 相关的僵尸网络，我们会进一步跟踪其内部指令，从而得以了解攻击的细节，包括攻击者是谁、受害者是谁、在什么时间、具体使用什么攻击方式。 最近俄乌局势紧张，双方的多个政府、军队和金融机构都遭到了DDoS攻...

Feb 25, 2022 · 12 min read

公有云威胁情报

公有云网络安全威胁情报（202201）

1. 概述 2022年的第一个月份，虽然没有爆发新的热门漏洞，且随着越来越多设备的Apache Log4j2漏洞被修复，12月开始的Apache Log4j2漏洞爆发也进入尾声，相关攻击源数量明显减少。但是，Docker Remote API未授权访问漏洞、美国飞塔（Fortinet）FortiOS未授权任意文件读取漏洞等旧漏洞的云服务器攻击源IP数量突然较12月大幅度增加。在第2部分，我...

Feb 21, 2022 · 11 min read

360 Netlab Blog - Network Security Research Lab at 360 © 2025

Powered by Ghost