DTA

用DTA照亮DNS威胁分析之路 (2)

suqitian
Jan 11, 2022 • 13 min read

--- 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，倒是有不少看起来合法知名的域名被拿来从事灰黑产，比如被传成互联网段子的www[.]whitehouse[.]com。

为了让简单且重要的DNS具备威胁分析的3个能力，Netlab在过去7年时间里建立了数量众多的数据库，包括但不限于：样本网络行为的Fdark、域名注册信息的Whois、域名备案信息的ICP、证书信息的Fcerti、各类统计信息的大网PDNS等等，不谦虚地讲，这些数据的规模和质量在国内应该都是数一数二的存在。正是有了这些数据库的辅助，加上Netlab多年分析大网DNS积累的经验，才让DTA具备了第二条核心理念“让威胁分析真正有效”。

那借助DTA让用户拥有网络威胁分析能力，究竟能带来什么好处呢?

场景

要说好处，我们先看现状的不足。

1、基于威胁情报触发的告警来发现威胁，其防护能力完全依赖于安全公司的情报输出，视野是有局限性的。

实践经验告诉我们，让样本、域名、IP等原始数据变成威胁情报的过程，是个智力密集型的过程，需要智力，知识，经验，技术相结合，其成本非常的高昂。这就决定了一个安全公司只能聚焦在某个自己擅长的领域内生产威胁情报，由此附带的影响就是：订阅情报的用户，视野也只能跟着局限在某个领域。记得在2020年底Netlab推出域名IOC（威胁情报）评估标准及评估数据服务之前，曾对多家公司的威胁情报进行过评估，确实发现不同公司发布的威胁情报，重合率仅约10%，而且重合部分大多集中在开源威胁情报。

进一步地，由于威胁情报生产的困难，天生自带分享门槛，因此一个用户如果同时订阅多家安全公司的威胁情报，成本是比较高的。另一方面，安全设备里运行着的百万级别威胁情报，真正在用户网络里命中并告警的可能不足一百，回报率又很低。高成本加低回报，让大多数用户只能默认做单项选择。

2、如果入侵行动是针对特定用户的高级威胁，安全公司恰巧能输出该威胁情报的可能性几乎为零。

这里的可能性几乎为零，并不是特指安全公司没有捕获到相关样本，没看见相关域名等等。而是指由于威胁情报生产的特性，必然让安全公司优先关注影响面广的事

件。高级威胁的事件，在没有资产属性辅助判断重要等级和证据链不完整的条件下，很难优先得到分析人员的关注并转化为威胁情报。

因此，把网络威胁分析能力赋能到用户网络的数据上，变被动防御为积极防御，让用户有能力输出属于自己的威胁情报，并结合公司资产的重要等级，评估威胁情报的优先级，应该是一件很有意义的事。

数据

为了更好的理解如何用DTA做网络威胁分析，我们先来看看它都有哪些方面的元数据。这好比厨师做菜前，先盘一盘手头都有哪些材料，好做到心中有数。

大致来说，DTA的数据分成3类。

类型	名称	备注
用户数据	-	DNS相关字段(仅列举本文用到的部分)
	域名	无
	Rdata	描述域名映射的资源，比如IP，CNAME等
	资产IP	请求域名解析的资产IP
	SLD	二级域
	...	
中间数据	-	基于用户数据预处理而得(仅列举本文用到的部分)
	资产网段	按A/B/C类网段划分资产IP
	服务器	根据资产访问行为判定为服务器
	内网域名	SLD归属部署DTA的公司
	域名流行度	结合大网PDNS和公司内网访问频率等数据计算得出的流行度
	...	
云端数据	-	360安全相关数据(仅列举本文用到的部分)
	IP Geo	IP地理位置信息
	ICP	域名备案信息
	Whois	域名注册信息

类型	名称	备注
	样本	网络访问行为数据，杀毒引擎检测结果等
	...	

功能

数据有了，接下来就是提出分析思路，然后借助DTA把思路转变成实操，最终找出潜在的威胁。本文抛砖引玉一个相对简单的例子：对服务器网段进行未知威胁分析。下面的4个小节，其实是呼应了“概述”里列举的3个能力，请读者自行对照。

思路

根据经验1：服务器网段是对外提供服务的，安全防护需求较高，有优先分析的必要；设备上运行的任务明确固定，因此向外的DNS请求单一，每天只发出几十个域名，有利于分析示例。相比办公区的个人设备，DNS请求复杂多变，每天会累计发出几百个不同的域名。

又根据经验2：由于国内网络管理较为严格，恶意域名映射的主机IP一般托管在国外；同时Alexa top 100k、内网域名、有ICP备案或者Whois注册人是可靠机构的域名也不太可能是恶意域名。

在图-1，我们把上述两个经验变成DTA的操作。看过文章1的读者，可能对这个界面有些印象，它就是“多个IoC”小节提到的“威胁分析”页面，在那里，我们只是把它当成查询后台数据库工具来用，查看有没有数据命中IoC。在这里，我们则是将分析经验变成规则来操作和分析数据集，期望从中找出符合预期的数据。在选好相关选项后，点击“应用”按钮，可以观察到约700台活跃服务器一周内共访问的1000+个去重域名，变成了只剩下58个待分析的线索。

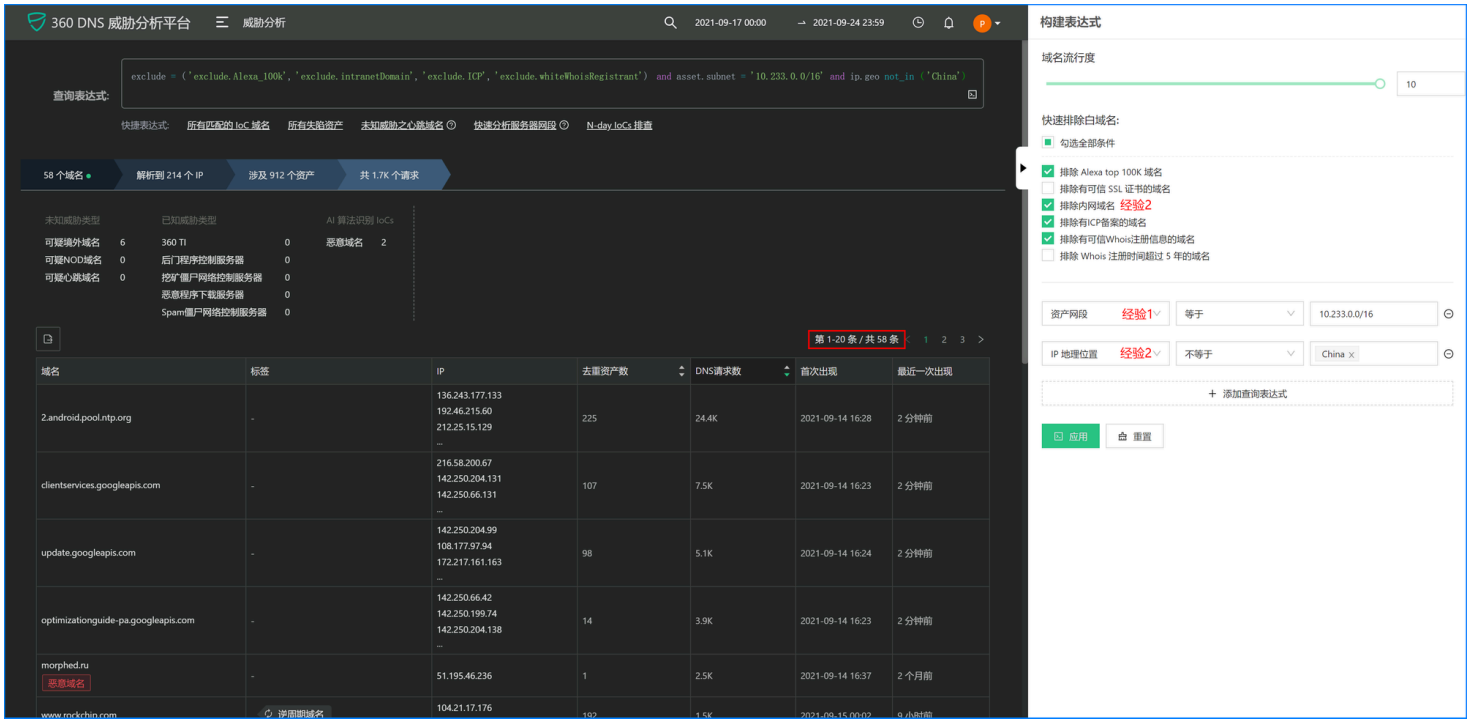

图-1 威胁分析能力1-1

改进

但58个域名还是偏多，理想的数量是小于等于20，原因一个是在后续的数据关联分析阶段，人可以快速处理关联结果，减少精力耗费；另一个原因是DTA的威胁情报图，启动一轮分析只会对前20条记录进行关联扩展，这样只需开启一次分析就可以:)。为减少待分析域名数量，需要进一步优化查询表达式。

改进经验1：把流行度高的域名过滤掉。因为流行度高的域名，大概率是白，如果是黑，也很容易被安全公司捕获并输出威胁情报，是未知威胁的概率低。因此把域名流行度调到8，至于为什么是8，不是7或者6，只能说是靠经验逐步调试得来，有点类似于厨师做菜时的少许盐~

改进经验2：图-1待分析域名列表包含了一些知名的站点，如“googleapis[.]com”，“gvt2[.]com” 等，通过域名SLD不等于表达式去掉。

图-2，线索只剩下20个了。观察输出列表，“morphe[.]ru” 和 “amnsreiuojy[.]ru” 有“恶意域名”红色标签，表明是命中了威胁情报，这不是我们关注的对象。因此，下一步，需要的是确认这18个线索里，有没有未知威胁。

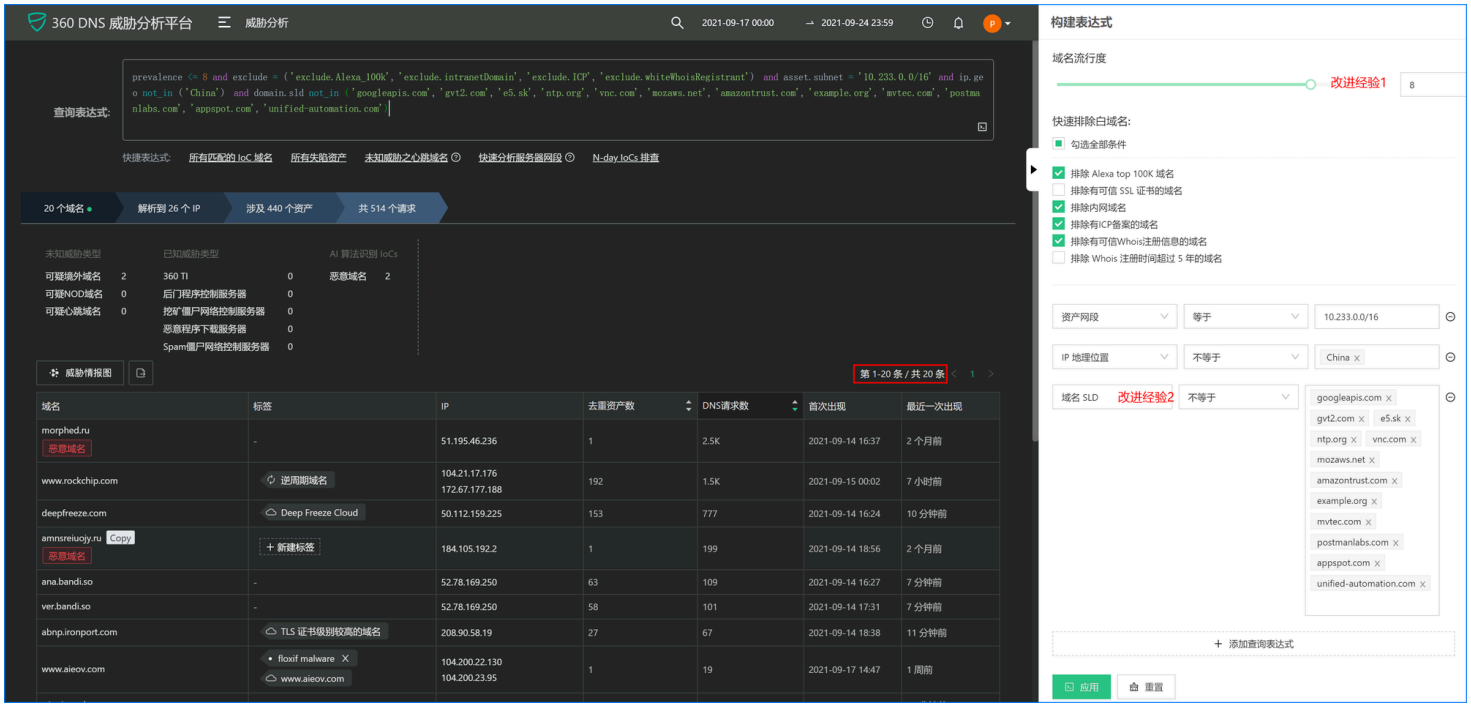

图-2 威胁分析能力1-2

确认

点击“威胁情报图”，借助云端的安全大数据来辅助判断这18个域名的黑白。要说明的是，判定域名黑白的方法有很多，这里的示例只是其中一种，并不代表非此不可。

图-3 威胁分析能力2-1

图-3里20个域名聚成了3类。左上角，有3个没命中威胁情报的域名*[.]deltaheavy[.]ru和2个已知的恶意域名聚在了一起，放大查看图-4通讯样本的详情，操作方法是用鼠标划停或点击样本框，均已标识为恶意样本，且为同一个家族。如果管理员能及时处理威胁情报给出的告警，这3个域名是能关联出来并清除掉的，所以它们不算是真正意义上的未知威胁。

图-4 威胁分析能力2-2

继续分析，我们找到了一个没有命中威胁情报的未知威胁 “www[.]aieov[.]com”(图-5)。通过搜索，属于一个已知的恶意家族Floxif。因此，这个未知威胁属于视野

局限类型的未知威胁，不是那种有针对性攻击的高级威胁。真正的高级威胁，在确认这一步需要补充更多的证据细节。

图-5 威胁分析能力2-3

分辨

在DTA系统上，通过观察资产在访问恶意域名时是不是有持续性，有没有可疑的伴生域名，源端口是随机的还是有规律的等行为细节，来分辨一个资产是不是被真实感染。

点击“威胁分析”页面的域名，跳转到域名详情页面。在右上角指定的时间范围内，通过绿色的流量图确认，有一个资产持续5天访问了该域名，说明恶意程序可能正在后台和C&C保持通信。真实感染的概率+1。多说一句题外话，如果想对单个域名做威胁分析，就在这个页面展开。

图-6 威胁分析能力3-1

点击左侧栏的资产“10.233.*.*”，跳转到资产详情页面。选择右侧的过滤条件，把白域名都排除掉利于分析。发现了一个伴生域名“5isohu[.]com”，和已知的恶意域名访问模式一致，通过查看样本网络行为，确认样本会同时访问两个域名。真实感染的概率+1。

图-7 威胁分析能力3-2

把左侧栏底部的滚动条拉到最右侧，点击“5isohu[.]com”最右侧的">"按钮，跳到“时间请求线”标签页，可以看到两个域名是成对出现的，且客户端端口呈随机分布，说明这是来自操作系统的请求，而不是虚拟机等测试环境的请求。真实感染的概率+1。如果有逆向分析样本的能力，还可以比较样本访问域名的逻辑是不是和左侧栏的时间间隔一致。至此，剩下的就是如何进行威胁处置了。

图-8 威胁分析能力3-3

结语

上述的操作过程，以DTA为操作台，将用户数据和360的安全大数据融合，找出了潜在的未知威胁。不过不知道读者有没有这样的感觉，即使是这个简单的入门示例，如果整个过程完全依赖人工一步步地从查找线索开始，到确认威胁，到最后的分辨真实感染，耗费的精力其实不小。

为了减少网络安全分析人员的工作量，DTA构建了多个模型，在后台自动完成了上述3个阶段的大部分工作，至于详情如何，下一篇介绍。

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 (1)

七年一剑，360 DNS威胁分析平台

See all 3 posts →

公有云网络安全威胁情报（202112）

1. 概述 云服务具备部署方便、资源灵活弹性、按需付费等优势，各类企业、政府、事业单位、高校和研究机构近年来都参与到了“上云”的潮流中。然而，随着越来越多各行各业的敏感数据“上云”，云安全问题的重要性和紧迫性也越发突出。近年来，全球云服务器被DDoS攻击、入侵、网站页面恶意修改、敏感数据泄露、加密勒索、恶意挖矿等安全事件频...

· Jan 19, 2022 · 14 min read

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...

· Dec 27, 2021 · 9 min read