

DTA

七年一剑，360 DNS威胁分析平台



kenshin

Oct 21, 2021 • 12 min read



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作中。过去7年多的安全研究，我们取得了非常多耀眼的成果：我们是360情报云最主要的情报供应团队之一，建立了国内首个也是最大的公开[PassiveDNS系统](#)，以及多个业内领先的Whois、证书、IP、样本等基础数据系统。我们诸多研究成果被国内外媒体转载报道，并多次在国际顶级安全会议发表演讲。我们在全球范围内率先披露了2位数以上有影响力的僵尸网络，并获得FBI的致谢，发现并命名的Satori僵尸网络的作者被美国国土安全局抓获并判刑，还有诸多不方便公开的实例不一而足。

凡是过往，皆为序章。

虽然过去7年我们一直以安全研究的形象出现，但这两年我们开始主动尝试产品化的探索。我们这么做不是为了KPI，而是渴望将我们在安全研究中积累的技术优势能够实实在在的应用到企业网络中，在更大维度内为客户网络安全直接贡献我们的力量，为客户的企业网络保驾护航。为了实现这个理想，我们从2019年开始研发

360 DNS 威胁分析平台 (DTA)，经过2年多反复打磨，今天正式对外介绍这款产品，这是360Netlab推出的首款商业产品，也是承载部门理想的产品。这个产品的定位不是传统的“大而全”，而是希望在 DNS 威胁分析这一个点上做得足够深、足够精，真正能替用户发现安全问题，为用户提供一个全新维度的安全工具。

360 DNS威胁分析平台

企业在网络安全体系建设中存在一个普遍现象，虽然采购了很多安全设备，但始终对自己的网络安全缺乏信心，究其原因，我们认为一个重要因素是客户无法“看见”网络内究竟在发生什么，有没有真正高可疑的威胁，如果有威胁能否进行有效的分析。从安全专家的角度来看，及时发现威胁，并能对威胁进行有效的分析和处置，是企业安全体系建设中至关重要的一环。**360 DNS威胁分析平台 (DTA)** 的产品初衷就是帮助客户从数据的维度看见自己的网络（security visibility），对自己的安全体系重拾信心。**360 DTA** 实现这一目标的核心理念是，让情报发挥应有价值，让威胁分析真正有效。



让情报发挥应有价值 . 让威胁分析真正有效

- 让情报发挥应有价值

威胁情报发展到今天已不再是一个新概念，很多安全厂商都建设了自己的 TIP，很多安全产品也都集成了威胁情报。但对于情报的应用，很多产品都有两个明显的缺陷。首先是机械的将威胁情报 IoC 视作黑名单，在流量中命中就告警。这会带来大量误报，并且产生的告警缺失上下文，用户既不明白报警的原因，也就不知道如何分析或者如何处置。另一个缺陷是目前主要的威胁情报源自云端，而真正来自企业本地独有数据、企业面对的真实威胁往往被忽视。大多产品的实现是命中某个 IoC 时，简单在 WEB 界面通过一个超链接跳转到云端 TIP 平台，但 TIP 上的情报信息是通用的，而客户本地的攻击是具体的，有针对性的，将情报和本地具体的请求行为，资产信息相结合来分析，才是对情报真正有价值利用。**DTA** 不仅有**360**

安全大脑海量威胁情报的赋能，同时作为情报生产团队，我们对于情报的价值有深刻的理解，并将情报应用到威胁检测、威胁分析的每一个环节。

- 让威胁分析真正有效

很多时候安全产品不被信任的一个重要原因是安全设备是一个黑盒子，客户只能被动接收设备的告警，但无论是基于规则的告警，还是基于算法或情报的告警，都是基于通用场景设计的，不是为某个具体企业或某次具体攻击行为设计的。而企业面临的威胁错综复杂，通用场景设计的规则往往很难有效发现一些定向攻击、高级攻击。DTA 以安全分析专家的视角去设计威胁分析功能，用户既可以简单直接查看系统经过多重环节筛选后的有效告警，更可以主动在产品内深入分析自己企业网络的流量。而用户看似简单的每一步分析操作，背后都有 DTA 海量情报和强大数据处理引擎的支撑，帮助用户降低威胁分析门槛，定位真实网络攻击。

The screenshot shows a web browser window for the '360 DNS 威胁分析平台'. The main content area displays a threat alert for incident #109, which has been detected as a highly suspicious恶意域名 (malicious domain). Key details include:

- 威胁类型:** AI 识别
- 创建时间:** 1 个月前
- 最近一次更新时间:** 3 天前
- 威胁等级:** 高

威胁描述: 域名判断的依据是利用VT和360大数据，提取多维度的特征计算黑白程度产生的。因未进行样本级别的逆向，多数情况下不能确定域名属于哪个具体的恶意软件家族。

处置建议: 通过AI模型发现的可疑恶意域名，虽然不能确定具体的威胁类型，但访问该域名的设备很可能处于风险中。可以尝试通过图分析引擎进行下一步分析，看能否关联到具体可疑的样本、域名、IP 或 URL。

公开分析: ...

IoCs (1)

IP	GEO	ASN
249.129.46.48	Reserved	Reserved
49.2.123.56	Australia	
118.5.49.6	Japan	4713 NTT_Communications_Corporation
253.157.14.165	Reserved	Reserved
77.4.7.92	Germany	6805 Telefónica_Germany
23.89.5.60	United States	18978 Enzu_Inc
188.5.4.96	Belgium	5432 Proximus_NV
54.76.135.1	Ireland	16509 Amazon.com,_Inc.
189.163.17.5	Mexico	8151 Uninet_S_A_de_C.V.
197.4.4.12	Tunisia	5438 Agence_Tunisienne_d'Internet

...共 10 条记录

域名情报

样本	杀毒引擎检测数	VT链接	样本标签	文件名	文件类型	端口
002d7a6547e483e03bf1a36aaadbab20	●●●●●	🔗	malware.pe...	Moon_3.0.1.exe,C:\Pr...	Win32 EXE	-
0a39a6da3f76abf97af24e1ba69e85b5	●●●●●	🔗	peexe,che...	0a39a6da3f76abf97af2...	Win32 EXE	-
0b267d3a87290fe7fd3d64dc87533ef4	●●●●●	🔗	peexe.bots...	NoEoIim.exe,C:\User...	Win32 EXE	-

管理告警

自动威胁行为分析: 存在恶意行为

状态: 待分析

分析结果: -

分配给: Nobody

全部评论 (0)

暂无评论，成为第一个评论的人！

记录威胁分析线索，添加分析结论

添加评论

应用场景

DTA 典型的应用场景是部署在客户企业内网，仅接入 DNS 流量就可以工作。通过分析内网 DNS 流量，检测内网潜伏的已知威胁、未知威胁和网络异常，精准定位失陷资产，并提供丰富的威胁线索和分析工具，帮助用户深入分析自己的网络流

量，定位高级攻击行为。但客户企业规模不同，安全建设阶段不同，关心的问题也会不同。我们概括了 DTA 三个主要应用场景，以及在这些场景下能为客户提供的核心价值。

- 安全体系成熟的客户

安全体系建设成熟的客户，往往面对的攻击也更加复杂，例如 0-day 攻击、定向攻击、APT 攻击，这类攻击最难于检测却最具威胁。DTA 的未知威胁检测能力、深入威胁分析能力，可以帮助客户及时识别这类高级威胁，快速进行处置。基于 DNS 流量的未知威胁检测一直是我们 360Netlab 的一个核心研究方向，我们在这个领域有超过7年的研究，积累了大量知识、经验、数据和算法模型，将这些积累应用到 DTA 的未知威胁检测模型中，让 DTA 具备了优秀的未知威胁、高级威胁检测能力。再加上功能强大的威胁分析系统，让客户可以深入分析网络内每一次请求，定位真实的攻击行为。

- 安全建设初期的客户

对于安全建设初期的客户，通常更关心降本增效，希望以较低成本解决尽可能多的安全问题，覆盖尽可能多的资产。DTA 仅依赖 DNS 流量就可以工作，而 DNS 流量有接入部署成本低、覆盖范围广的特点。企业内几乎所有联网设备都会发出 DNS 请求，而 DNS 流量仅占企业内网总流量的 1% - 1%，但根据美国安全厂商 [Palo Alto Networks 的研究](#)，超过 80% 的恶意软件在和 C2 通信阶段会使用 DNS 协议，因此基于 DNS 流量的威胁检测是一个简单又行之有效的方式。再加上 360 作为国内最大的网络安全公司，在安全数据、云端情报建设上有遥遥领先的优势，有了 360 安全大脑的赋能，客户通过部署 DTA，可以较低成本快速建立起基础的安全运营能力。

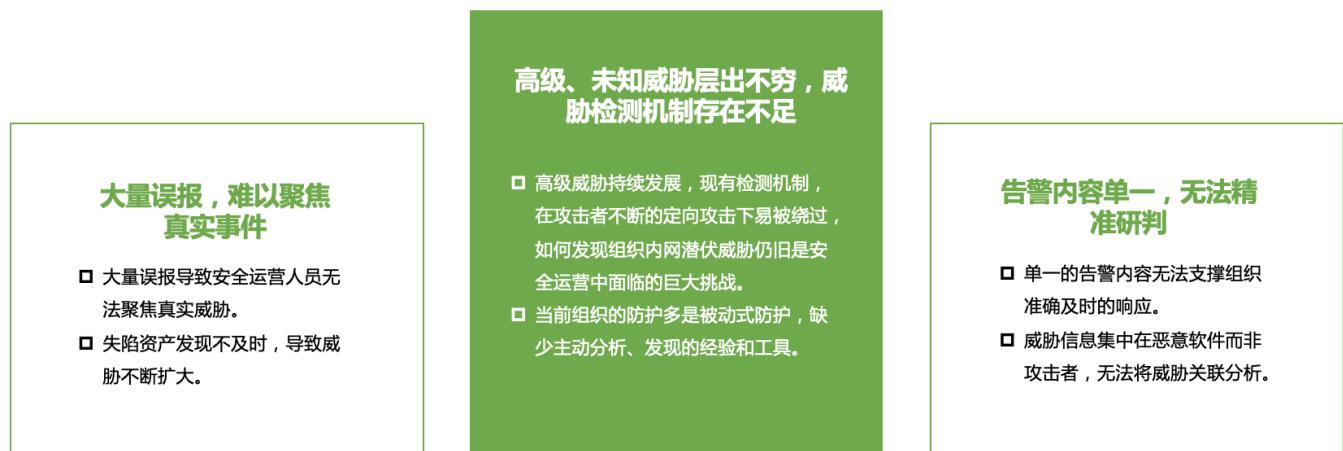
- 大流量监管

对于城市安全运营部门或行业监管部门，有城市出口流量或行业流量监管的需求。这类场景通常会面临两个巨大的挑战，首先是流量异常复杂，真实威胁流量混杂在绝大多数正常的流量中，很难准确识别。另一个挑战是这类场景通常数据量巨大，对系统的处理性能和分析能力是非常大的考验，协议层越往上，分析难度越大，容易造成一个常见的困境：虽有海量数据，但无从下手，有价值数据被淹没。DTA 在大流量威胁分析方面经验丰富，我们 360Netlab 运营多年的 [DNSMon 系统](#) 每日对千亿级别的大网 DNS 流量进行分析，在无任何先验知识的情况下，每日输出

数千条高风险恶意域名，并通过[360 安全DNS](#)为国内约2000万用户提供安全解析服务。此外 DTA 整体采用分布式系统设计，所有模块均可根据流量大小水平扩展，并能根据客户基础设施不同，运行于私有云、公有云、容器云平台，可有效支持大流量监管的场景。

三大创新

长久以来，很多安全设备一直因为大量漏报、误报，被广受诟病。每天动辄数千、数万的报警，让安全运营人员疲于奔命，真实威胁隐藏在大量误报中无法被有效聚焦。而大安全时代，攻击手段越来越高级，企业面对的安全威胁越来越复杂，对于高级威胁、未知威胁检测机制存在严重不足。



我们对这款产品的自信，源自我们通过一些技术创新，优化了一些其它产品没有很好解决的问题。这些创新具体体现在未知威胁检测、精准告警、高效威胁分析三个方面。

核心功能

- 威胁检测

通过高质量情报和多个创新检测模型，检测内网的已知威胁、未知威胁和网络异常，精准定位失陷资产。其中未知威胁检测是 DTA 的亮点功能，可以帮助用户及时发现高级威胁，快速进行处置。

- 威胁分析

安全专家设计的威胁研判、威胁分析系统，将企业 DNS 流量掰开了、揉碎了进行重新组合、标注、并将本地数据与云端情报深度融合，让用户可以主动在 DTA 产品内深入分析自己企业网络的流量，定位真实攻击行为。

- 可视化

客户流量接入 DTA 后，系统自动对流量进行建模，通过可视化方式，为企业的网络建立全局视野。并通过特征和行为分析算法，自动识别数字资产，在不需要人工维护的情况下实现数字资产和风险可视化。

初露锋芒

过去一年多时间，DTA 一直作为 360 自身安全运营的一部分，在 360 企业内网试运行，在实战中不断打磨自己，也在实战中开始展露自己，并成功发现了多起真实威胁。360 作为国内安全建设最为健全的公司之一，如果 DTA 能发现多起真实威胁，相信部署到我们的客户网络后，同样能帮助我们的客户提升安全运营能力，加强纵深防御深度。作为一款新产品，DTA 已经展现出了一些亮点，但离我们的目标还有很大距离，期待和我们的客户一起，以客户的真实需求、面对的真实威胁为指引，共同将 DTA 打造成一款更加优秀成熟的安全产品。

商务咨询，联系 xuyinghan@360.cn



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 (3)

用DTA照亮DNS威胁分析之路 (2)

用DTA照亮DNS威胁分析之路 (1)

Botnet

一个藏在我们身边的巨型僵尸网络 Pink

本文完成于2020年春节前后，为维护广大最终消费者的利益，一直处于保密期无法发表。近日 CNCERT 公开披露了相关事件，令本文有了公开契机。在保密期的这段时间里，Pink 也出现一些新的小变动，笔者筛选了其中一部分放到“新动向”章节，供其他同仁共同追踪研究。概述 2019年11月21日，安全社区的信任伙伴给我们提供了一个全新的僵尸网络...

0-day

Mirai_ptea_Rimasuta variant is exploiting a new RUIJIE router 0 day to spread

Overview In July 2021 we blogged about Mirai_ptea, a botnet spreading through an undisclosed vulnerability in KGUARD DVR. At first we thought it was a short-lived botnet that would soon disappear so we just gave it a generic name. But clearly we underestimated the group behind this family, which



[See all 3 posts →](#)



• Oct 26, 2021 • 23 min read



Sep 28,
2021

10 min
read