

**suqitian**

Botnet

A new botnet Orchard Generates DGA Domains with Bitcoin Transaction Information

DGA is one of the classic techniques for botnets to hide their C2s, attacker only needs to selectively register a very small number of C2 domains, while for the defenders, it is difficult to determine in advance which domain names will be generated and registered. 360 netlab has long focused



• Aug 5, 2022 • 13 min read

Botnet

DGA家族Orchard持续变化，新版本用比特币交易信息生成DGA域名

DGA是一种经典的botnet对抗检测的技术，其原理是使用某种DGA算法，结合特定的种子和当前日期，定期生成大量的域名，而攻击者只是选择性的注册其中的极少数。对于防御者而言，因为难以事先确定哪些域名会被生成和注册，因而防御难度极大。360 netlab长期专注于botnet攻防技术的研究，维护了专门的DGA算法和情

报库，并通过订阅情报的方式与业界分享研究成果。近期我们在分析未知DGA域名时发现一例不但使用日期，还会同时使用中本聪的比特币账号交易信息来生成DGA域名的例子。因为比特币交易的不确定性，该技术比使用时间生成的DGA更难预测，因而防御难度更大。该技术发现于一个名为Orchard的botnet家族。自从2021年2月份首次检测到该家族以来，我们发现它至少经历了3个版本的变化，中间甚至切换过编程语言。结合长期的跟踪结果和其它维度的信息，我们认为Orchard会是一个长期活跃、持续发展的botnet家族，值得警惕。本文将介绍Orchard的最新DGA技术，以及它这3个版本的发展过程。本文要点如下：

- * Orchard是一个使用了DGA技术的botnet家族，核心功能



· Aug 5, 2022 · 18 min read

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



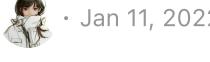
· Feb 24, 2022 · 10 min read

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

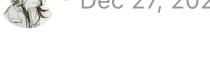
的线索；3、分辨资产被真实感染的能力。只有确认真实感染，才能保证后续的威胁处置动作有成果。按：由于DTA也实现有“已知”威胁分析功能，但其用法和本文描述的操作细节相差甚远，为避免混淆，特此说明一下本文所有威胁分析的用词，都是指“未知”威胁分析。在上一篇文章，我们提到DNS日志的优点是简单且重要。但正是福兮祸所倚，简单这个优点，从威胁分析的角度来讲它又成了最大的缺点，因为这意味着日志包含的有效信息少。具体来讲，一次DNS请求和回应所解析出来的内容，除去极个别喜欢炫技的特意使用有区分度的词语，比如hackerinvasion[.]f3322.net, hackattacks[.]org等，大多数日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



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Netlab 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



en

DNSMon: using DNS data to produce threat intelligence (3)

Background This article is the third in our series of articles introducing DNSMon in the production of threat intelligence (Domain Name IoC). As a basic core protocol of the Internet, DNS protocol is one of the cornerstones for the normal operation of the Internet. DNSMon, which was born and raised



DNSMon

DNSMon: 用DNS数据进行威胁发现(3)

--- Linux, Windows, Android, 一个都不能少 背景 本文是介绍DNSMon在生产威胁情报(域名IoC)系列文章的第三篇。DNS协议作为互联网的一项基础核心协议，是互联网得以正常运行的基石之一。在祖国960万平方

公里的土地上，那一张纵横交错的数据网络里，每一秒都有数万亿计的DNS数据包在高速穿梭着，它们或来自于机房的服务器，或来自于办公室的电脑，或来自于我们身边的手机，或来自于场景繁多的IoT，总之DNS无处不在。生长于斯的DNSMon，依托DNS协议的基础性，天然具备宽广的视野，对那些发生在不同行业或不同平台的安全事件，都能有所涉猎。在DNSMon科普系列的前两篇博文中，第一篇提及的Skidmap是感染Linux平台的云主机；而第二篇提及的一组域名是网吧的Windows平台被感染后发出的；本文则是一个涉及Android平台的案例。如果仔细阅读文章并理解其中内容，可以看到DNSMon在面对3个差异巨大的平台时，所使用的知识点或者说规则并没有根本性的变化，几乎做到了无差别预警。对未知威胁的拦截 最近，我们注意到DMSMon从

2021-01-10



Feb 8, 2021 · 10 min read

DNSMon

DNSMon: 用DNS数据进行威胁发现(2)

----DNSMon抓李鬼记 背景 本文是介绍DNSMon在生产威胁情报(域名IoC)系列文章的第二篇。为了对抗安全人员的分析，钓鱼域名是恶意样本经常采用的一种技术手段。从字符组成和结构上看，钓鱼域名确实具有混淆视听的功效，但对于DNSMon这种具备多维度关联分析的系统来说，模仿知名公司域名的效果则适得其反，因为这样的域名一旦告警，反而更容易引起分析人员的注意。本案例从一组疑似钓鱼域名出发，逐步介绍DNSMon是如何利用whois, ICP备案，域名解析内容和图关联等信息，让一组干瘪的域名逐渐一点点丰富起来直至最后恶意定性的。意料之外的是，随着线索的展开，我们发现这是一起失陷设备数量巨大的安全事件，从我们的数据测算，感染规模远超100w设备。为此，我们进行了较为细致的逆向分析和回溯，但限于篇幅，样本分析细节及其家族演变，将在后续再另起一篇介绍。通常威胁分析普遍的惯例是先知道样本恶意再逆向，有时根据DNS数据估算感染规模。这次DNSMon系列文章里揭示的，更多是先根据DNS数据发现异常并定性，再进一步探寻还原事件真相。即从先逆向再统计，变成了先统计再逆向。这个顺序



Dec 31, 2020 · 14 min read

Import 2022-11-30 11:16

双枪团伙新动向，借云服务管理数十万僵尸网络

本文作者：jinye, JiaYu, suqitian, 核心安全部研究员THL 概述 近日，我们的域名异常监测系统 DNSMon 捕捉到域名 pro.csocools.com 的异常活动。根据数据覆盖度估算，感染规模超过100k。我们通过告警域名关联到一批样本和 C2，分析样本后发现是与双枪恶意程序相关的团伙开始新的大规模活动。近年来双枪团伙屡次被

安全厂商曝光和打击，但每次都能死灰复燃高调复出，可见其下发渠道非常庞大。本次依然是因为受感染主机数量巨大，导致互联网监测数据异常，触发了netlab的预警系统。本报告中我们通过梳理和这些URL相关的C2发现了一些模式，做了一些推测。我们观察到恶意软件除了使用百度贴吧图片来分发配置文件和恶意软件，还使用了阿里云存储来托管配置文件。为了提高灵活性和稳定性，加大阻拦难度，开发者还利用百度统计这种常见的网络服务来管理感染主机的活跃情况。同时我们在样本中多次发现了腾讯微云的URL地址，有意思的是我们在代码中并没有找到引用这些地址的代码。至此，双枪团伙第一次将BAT三大厂商的服务集成到了自己的程序中，可以预见使用开放服务来管理僵尸网络或将成为



· May 23, 2020 · 21 min read