DNSMon

360netlab上线域名IOC（威胁情报）评估标准及评估数据服务

Zhang Zaifeng
Nov 2, 2020 • 4 min read

版本一：程序员版

一直以来，由于高门槛，安全圈里对威胁情报质量没有一个很好的评估手段，

> *PR狠的公司的威胁情报就更好么？*
> *名头响的公司的威胁情报就更好么？*
> *使用了机器学习人工智能这些热词的威胁情报就更好么？*
> *拿了一堆排排坐吃果果的奖的公司的威胁情报就更好么？*

难有人能给个说法，所以最后我们看到用户只能回到一个聊胜于无的方法，哪家的威胁情报的总数多哪家就好，出现的告警次数多哪家就好！
这个方法其实巨坑，举个?:

> *A和B厂家提供两份威胁情报，A有10万条IOC，B有5万条IOC。*
> *A的10万条IOC在实际网络中总命中IOC不到1000条，产生了20000次告警。*
> *B的5万条IOC在实际网络中命中IOC15000条，也产生了20000次告警。*
> *你愿意选择哪个？*

那咋办?
经过一段时间的准备，我们推出来了个一个公益的评估标准，而且还免费提供大网的实际评估数据从而让客户有真实数据评估。

我们这么干是为啥？ 是不是有啥阳谋，要怎么收数据之类的？（答案，没有，看看我们的正经页面就能懂）

另外我们很欢迎有经验的用户提供反馈修正等，对于采用的反馈合并进入评估标准后，我们会在评估手册中列出相应的贡献者名单。

版本二：项目经理版

背景简介

IOC（威胁情报）评估是威胁情报采购，使用过程中极为重要的一个环节。对其进行科学，透明和可量化的评估是整个威胁情报产业一个重要的组成部分。

鉴于目前市场上缺乏相应的评估标准及评估服务，360netlab基于多年来实网数据分析经验以及丰富的安全分析积累，提出了《域名IOC（威胁情报）评估标准》的第一版——“域名IOC评估19条”——包括11条静态评估标准及8条动态评估标准。

为了更便捷的使用该标准，我们提供了域名IOC（威胁情报）评估标准的线上版本。

服务内容

考虑到无论是生产方还是消费方，IOC均为其最核心的资产，从数据安全的角度出发，360netlab不提供对用户IOC的直接评估服务。我们提供可以实操的评估手册和评估过程所需的基础数据，用户可以按照评估手册自行完成整个评估过程。

评估手册

首先，我们特提供了域名IOC（威胁情报)评估的操作手册，手册中的每一项都有详细的解释以及建议的操作方法，不同的IOC（威胁情报）相关方可根据手册进行自评和验证。

需要说明的是，评估标准是一个不断改进和完善的过程。我们非常欢迎业界同仁对域名IOC（威胁情报）的评估提供反馈意见。对于任何科学有益的建议，我们都会合并进入评估标准，并清晰注明相应的贡献者，作为《域名IOC（威胁情报)评估标准》的后续版本进行发布。

评估数据服务

其次，考虑到不同用户在进行域名IOC（威胁情报）评估时的数据门槛，尤其是动态评估过程中缺乏基础数据以完成评估，360netlab提供了“域名IOC评估数据服务”。

该服务对需要使用基础数据进行IOC（威胁情报）动态评估服务的用户免费提供一定时间段的原始数据。需要的用户可以通过我们的评估网站 进行申请。

最后，关于IOC（威胁情报）评估服务的详细内容以及更多其他的内容，欢迎访问我们的评估网站 https://assess-ioc.netlab.360.com 。

DNSMon

俄乌危机中的数字证书：吊销、影响、缓解

商业数字证书签发和使用情况简介(删减版)

An assessment of Non-Authorized Domain Name Resolution provided by DNS Resolution Service Provider

See all 28 posts →

HEH Botnet, 一个处于开发阶段的 IoT P2P Botnet

概述 近期 360Netlab 未知威胁检测系统捕获到一批未知恶意家族的样本，这一批样本支持的 CPU 架构有 x86(32/64), ARM(32/64), MIPS(MIPS32/MIPS-III) 以及 PPC，经过我们分析，将其命名为 HEH Botnet。HEH 是一个由 Go 语言编写的 IoT P2P Botnet，它的 P2P 协议不基于公开的任何 P2P 协议，而是自研协议。HEH 现阶段会通过...

· Nov 9, 2020 · 10 min read

HEH, a new IoT P2P Botnet going after weak telnet services

Overview Recently, 360Netlab threat detection system captured a batch of unknown samples. The CPU architectures supported by this batch of samples are broad, including x86(32/64), ARM(32/64), MIPS(MIPS32/MIPS-III) and PPC, it is spreading through brute force of the Telnet service on ports 23/2323,...

· Oct 7, 2020 · 8 min read