登录

【原创】增加网络中5个黑暗区域的"可见度"

threatfinder / 2016-10-25 23:53:00 / 浏览数 2139 安全技术 技术讨论 顶(0) 踩(0)

0x00 用户对用户活动

1. 描述:

虽然full-packet检测是安全架构很重要的一个部分，但是full-packet检测不是被设计成监控网络内部的所有主机间通信的流量。网络中捕获每个包的流量所产生的体积会严重

插图1

1. 解决方案:

NetFlow可以增加通过访问层的用户-用户的可见度，而且不影响网络性能。因为NetFlow的数据拼成一个flow的一小部分，这里有其路由到收集点进行分析而少得很多的性

增加用户对用户的可见度，对于了解恶意软件怎么通过网络传播尤为重要。基于行为的分析对于检测恶意软件相关联的流量patterns非常有用。

0x01 特殊的网络设备

1. 描述

Endpoint终端安全客户端可以运行在一些流行的桌面和服务器操作系统上。专业设备:例如多功能打印机、POS终端、ATM取款机以及物联网设备等，很少部署Endpoint终端

插图2

1. 解决方案:

基于NetFlow的分析可以有效的使特殊网络设备增加"可见度"，而无需中断主要设备。使用异常流量检测方式可以解决这个问题。

0x02 加密流量

1. 描述

加密通信是另外一个在网络中的黑暗区域。越来越多的C&C服务器和被入侵的设备的指挥和控制进行加密，以避免被发现。面临的挑战是:你怎么发现不知道内容是什么的情

插图3

1. 解决方案

类似生活中电话的例子，它"不一定"知道你说写了什么，进而确定恶意活动正在进行。它是利用一些Meta信息来获取一些关联的数据来进行分析。具体元数据的可怕性可以参
23上的议题《Applied Intelligence Using Information That's Not
There》。在网络的世界中的Meta信息就是源地址、目的地址、时间戳、传输的数据量、源端口、目的端口以及其他NetFlow中的信息点，进而可以标识出通信中的威胁而不

真实的应用行为分析案例是，在一个典型的网络中，数据泄露可以使用基于异常行为的检测行动。通常，一个内部主机被作为基线通常只与内部服务器通信，但是突然开始与

0x03 远程网络

1. 简介

因为跨网络办公地点的增加，安全相关的成本也迅速增加。你必须检测广域网的流量或者你必须在边界实现本地检测设备。即使在远程办公地点部署了边界检测，你可能依然

1. 解决方案

通过使用WAN和中心收集节点的backhaule（回程链路），可以解决这个黑暗区域。一旦攻击者渗透到网络是，他们可能去横向渗透本地网络分段中的其他主机。如果没有

0x04 内部数据中心

1. 描述

为了解决大数据量的流量从东向西快速经过最深层的数据包检测设备，安全架构师通常把深度包检测部署在数据中心的边界上。数据中心可见度的问题就是获得一台主机上两

2.解决方案

虚拟机可视化问题既然可以通过NetFlow来解决。大多数的现代的Hypervisors支持NetFlow流量监测。

0x05 参考

1. Advanced Threat Detection: Gain Network Visibility and Stop Malware

https://www.lancope.com/sites/default/files/5-Dark-Places.pdf

1. Cisco Cyber Threat Defense 2.0 Design Guide

http://www.cisco.com/c/dam/en/us/td/docs/security/network_security/ctd/ctd2-0/design_guides/ctd_2-0_cvd_guide_jul15.pdf

1. Defcon 23 Applied Intelligence_ Using Information That's Not There

https://media.defcon.org/DEF%20CON%2023/DEF%20CON%2023%20presentations/Michael%20Schrenk%20-%20UPDATED/DEFCON-23-Michael-Schrenk-Ap

1. WAN回程链路

http://baike.sogou.com/v10974425.htm

1. 0 条回复
   - 动动手指，沙发就是你的了！