HongKe 虹科

PROFITAP

白皮书：

Profishark 1G使用案例分析

Wireshark 英雄系列

VISIT WWW.hongwangle.com

BRAD PALM

OPERATOR AT BRUTEFORCE LLC

Brad是一个问题解决者和融合性思维者，他期待着在物理和虚拟世界之间架起桥梁的挑战。他在分析和驾驭采用技术时固有的IT风险方面具有很高的技巧，他有动力与动态、快节奏、高绩效的团队一起工作.Brad正在经营BruteForce，这是一家数字安全和网络分析咨询公司。他们的解决方案堆栈包括用DevOps原则构建弹性架构，对这些设计进行压力测试和突破，以不断改进和硬化它们，然后积极防御和猎取它们的环境以持续完成任务。

专业知识：

- *DevOps/Security Engineer focused on IT solutions enabling resiliency.*
- *Passionate about build, break, hunt!*

BRAD@BRUTEFORCE.IO

LINKEDIN.COM/IN/BRADPALM/

背景

在进行数字取证和事件响应(DFIR)时，拥有高质量的网络测试接入端口(TAP)的重要性已经在Profitap的一份名为“特种部队专用工具：利用网络空间中的实时威胁”的白皮书中得到了阐述。除了白皮书中介绍的要点之外，我还想提供最近的一个使用案例，其中ProfiShark 1G在决定系统的受损方面发挥了关键作用。

最近，我在对一个环境进行威胁检测时，遇到了一个主机系统，它所呈现的妥协指标（IOC）非常令人信服。在对主机进行了一系列测试（如：chkrootkit、lynis、rkhunter）后，所有工具的结果都是报告系统是干净的，没有被入侵。这时，你就会面临这样的决定：是排除主机系统被入侵的可能性，还是开发一个后续测试，以便对系统进行更精细的观察。

下面的用例分析将深入探讨ProfiShark 1G如何为您提供所需的细粒度视图来检查网络流量，并使您能够确定是否受到危害。我用描述产品价值主张的方式来进行分析。我使用这种方法，因为这是我比较和评估产品的方式，以便将其纳入我个人的DFIR袋中，或纳入我解决问题的技术 "解决方案堆栈 "中；而且它使我能够快速地了解基本事实。就本用例而言，我发现图1所示的ProfiShark 1G和ProfiShark 1G+都同样适用于DFIR工作，当我提到ProfiShark 1G时，它也可以理解为 "ProfiShark系列产品"。

图1: ProfiShark 1G和 1G+ 比较

Profishark 1G解决什么问题？

纵观全局，ProfiShark 1G 可以让您进行网络分析，包括三个大的方面 -- 故障排除、优化和取证。所有这三个领域都严重依赖于网络流量的基线，然后确定哪些是可疑或 "有趣 "的流量。ProfiShark 消除了执行这些基线的障碍，因为它是专门为网络工程师 /安全工程师设计的。

关于所介绍的使用案例，ProfiShark 1G可以让您通过协助基于网络的 " 交叉视图 "Rootkit分析来实现对主机系统的精细观察。基于网络的交叉视图分析包括从两个不同的有利点观察网络连接。一个有利点是从主机系统的用户空间角度出发。另一个有利点是从无偏的角度出发，在这个角度上，Rootkit无法操纵呈现给分析人员的信息。然后，你比较从这两个有利点收集到的结果，如果有任何网络连接差异，你就可以断定存在rootkit（这是一个简化的启发式方法，因为解决所有边缘情况所需的逻辑超出了本文的范围）。当ProfiShark 1G插入到网络路径中，毗邻主机系统的网络接口控制器(NIC)时，它提供了无偏优势位置，并捕获到/来自主机系统的数据包。

刚开始对主机系统进行审问时，我上传了两个常用的rootkit检查工具，并运行它们。rkhunter扫描的部分结果如图2所示，chkrootkit扫描的部分结果如图3所示。这两个工具的结论都是不存在rootkit。

```
[13:48:57] System checks summary
[13:48:57] ====================
[13:48:57]
[13:48:57] File properties checks...
[13:48:57] Required commands check failed
[13:48:57] Files checked: 124
[13:48:57] Suspect files: 5
[13:48:57]
[13:48:57] Rootkit checks...
[13:48:57] Rootkits checked : 431
[13:48:57] Possible rootkits: 0
[13:48:57]
[13:48:57] Applications checks...
[13:48:57] All checks skipped
[13:48:58]
[13:48:58] The system checks took: 1 minute and 42 seconds
```

图2：rkhunter扫描输出的结果

```
ROOTDIR is `/'
Checking `amd'... not found
Checking `basename'... not infected
Checking `biff'... not found
Checking `chfn'... not found
Checking `chsh'... not found
Checking `cron'... not infected
Checking `crontab'... not infected
Checking `date'... not infected
Checking `du'... not infected
Checking `dirname'... not infected
Checking `echo'... not infected
Checking `egrep'... not infected
Checking `env'... not infected
Checking `find'... not infected
Checking `fingerd'... not found
Checking `gpm'... not found
Checking `grep'... not infected
Checking `hdparm'... not found
Checking `su'... not infected
Checking `ifconfig'... not infected
Checking `inetd'... not tested
Checking `inetdconf'... not found
Checking `identd'... not found
Checking `init'... not infected
Checking `killall'... not infected
Checking `ldsopreload'... can't exec ./strings-static, not tested
Checking `login'... not infected
Checking `ls'... not infected
Checking `lsof'... not infected
Checking `mail'... not found
Checking `mingetty'... not found
Checking `netstat'... not infected
Checking `named'... not found
Checking `passwd'... not infected
Checking `pidof'... not infected
Checking `pop2'... not found
Checking `pop3'... not found
Checking `ps'... not infected
```

图3：部分chkrootkit扫描输出的结果

我对这些工具提供的结论并不满意，觉得有必要对主机系统做进一步分析。现在开始前面介绍的跨视角分析技术。对于用户空间的有利位置，我使用了netstat工具，它可以打印出网络连接到命令行。我使用以下标志$ netstat -plant来检查活动的TCP套接字。这个命令只输出一个活动会话，那就是我的SSH会话，用于远程连接主机系统。

为了无偏优势位置，我从主机上拔下Cat5e以太网电缆，将ProfiShark 1G TAP插入网络设备串，然后将Cat5e电缆重新连接回主机。这就为我提供了有利位置，能够验证用户空间netstat命令是否给我提供了主机系统上网络连接的准确描述。

在Wireshark中启动网络捕获，并让它运行几分钟后，实时捕获描绘了一个不同的情况，并显示有一个额外的SSH会话指向系统无法与之交谈的外部IP地址。我再次运行netstat命令，确认这个会话没有显示在用户空间优势点中。现在，我已经掌握了这些信息，我可以放心地把这个系统拉出线，并开始必要的事件响应步骤，使其恢复到已知的良好状态。

Profishark 1G创造了什么价值？

如果你接受了Rootkit检查工具的结果，你就会允许一个被入侵的系统在你的网络上持续存在。现在，要确定攻击者的动机是极具挑战性的，尤其是当你的目标是缩短检测IOC的时间和缓解IOC的响应时间时。然而，我不建议你让你的网络成为一个培养皿，在那里你可以观察最新的对手在你的网络中移动，这样你就可以对他们进行动机和行为分析（这项有趣的工作是由研究人员用迷人的蜜罐/主动防御环境来完成的）。相反，通过观察对手活动的最新趋势，可以得出这样的结论：如果你允许威胁在你的环境中持续存在，他们可能一直在寻找快速赚钱（例如，勒索软件），收获你的主机系统资源以挖掘加密货币（例如，加密劫持），或者如果你是一个拥有一些有趣的研究或知识产权的组织，则可能会长期挖掘（例如，高级持续威胁）。

通过采取彻底的方法，并使用ProfiShark 1G进行基于网络的交叉视图分析，您可以回答一个关键问题，求得答案--我是否受到威胁？

Profishark 1G解决方案的影响是什么？

如前所述，ProfiShark 1G消除了进行基线的障碍。它通过跨平台、小外形、没有其他RJ-45聚合TAP的瓶颈考虑来实现。案例--我已经在Windows和Linux操作系统上安装并使用了ProfiShark 1G，ProfiShark比我的iPhone 6还要小，我通过在不丢弃数据包的情况下向两个方向发送全线速流量，对ProfiShark的捕获能力进行了压力测试。

早些时候，我提到ProfiShark 1G和1G+在我介绍的使用案例方面是可以互换的，我想收回这一点。它们不容易互换的情况是在考虑时间标记时。图4所示的ProfiShark 1G+增加了从天空中的精确时间服务器（也称为全球定位系统（GPS））提取时间的额外功能。当您需要在地理上分散的地点进行拍摄，并希望合并或交叉引用这些采集数据以进行深入分析时，这个功能就显得尤为有趣。

同样令人信服的是，你可以使用这种精确的第三方时间同步作为一种方式来增加网络捕获的有效性，如果它必须作为直接证据使用，作为法律程序的一部分。现在，你不必在部署到那些不同的采集点之前，依赖时间的变化或试图同步多个采集盒。

图4: ProfiShark 1G+ 带有GPS天线

结论

通过使用ProfiShark 1G网络TAP，我得以确认系统中确实有一个rootkit，它正在混淆用于恶意通信的网络插口。这些数据包从来不会说谎，当对TAP（主机网卡外部）捕获的流量和主机系统内置的网络工具进行一对一的对比时，它们表明存在被屏蔽的恶意活动。当出现这样的情况，你无法再信任主机操作系统时，你就必须利用一个可信的第三方工具来审问受感染的系统。

底线--作为一名负责保持网络运行和安全的 IT专业人员，我对进入我的网络故障排除/网络取证工具包的工具非常挑剔。 ProfiShark 1G 或1G+绝对已经在我的工具包，或者说 在我的口袋里赢得了一席之地。

产品信息

关注我们

HongKe 虹科

广州虹科电子科技有限公司

需要详细信息？请通过sales@hkaco.com

联系我们电话: 400-999-3848

广州 | 北京 | 上海 | 深圳 | 西安 | 武汉 | 成都 | 沈阳 | 香港 | 台湾 | 美国