阻止恶意软件 — 在它连接到服务器发出警报之前。

检测无声的、周期性的信息。这表明设备已受到入侵被攻破。那些您的防病毒软件永远发现不了的威胁。

24/7	≤1 小时	6	10
被动监控	告警响应	检测层级	实时仪表盘

问题

您的防病毒软件无法捕捉到它

现代恶意软件极少自我暴露。它静默安装,然后通过短小、规律、加密的消息向操作者通信 — 这就是 **信标**。一旦确认存在活跃的命令通道,攻击者便会进一步行动:横向移动、数据外泄、部署勒索软件。

传统防御依赖文件与签名匹配。信标看上去并不像恶意软件 — 它们看起来像后台流量,而这正是它们的设计意图。

勒索软件预备阶段

攻击者在加密前会先确认访问、绘制网络拓扑 — 信标是事态出错的最初信号。

远程访问木马

RAT 每隔数分钟连接一次。签名扫描看到的是正常进程;信标分析看到的是模式。

隐蔽数据外泄

以固定间隔发送的小且一致的数据包,对基于流量量级的异常检测是不可见的。

供应链植入

可信软件可能被植入恶意代码。即便看似合法的流量,也必须依据周期性行为予以识别。

解决方案

基于行为的网络监控

Beacon Butty 部署在您的局域网与互联网之间,跟踪并对每条连接评分 — 不阻断、不延迟任何数据包,对网络性能零影响。

它不依赖已知恶意签名匹配,而是衡量 *行为*:连接的规律性、负载大小的一致性、目的地特征的异常程度。这些统计模式即便在加密与混淆下依然有效。

B

信标评分

RITA v5 按周期性、抖动、数据包大小与持续时间对每台主机评分。

I

入侵检测

Suricata IDS 实时扫描数千条签名,智能过滤噪声。

N

网络情报

TLS/DNS 异常、地理位置、ASN、Tor 出口节点与域名熵值。

A

资产清单

通过 DHCP、ARP 与 Nmap 自动发现局域网设备,含操作系统与开放端口。

F

误报控制

基于 MAC 的注册表抑制已知良性设备与域名。

!

即时告警

支持 Slack 通知,可按类型启用/停用,并按告警设置抑制窗口。

六层检测流水线

1 被动数据包捕获 `Zeek 8`

Zeek 在内部接口被动监控全部局域网流量,对吞吐量零影响。每条 TCP/UDP 连接均记录完整元数据:时间戳、字节数、状态、持续时间与 TLS 握手详情。

2 信标评分引擎 `RITA v5`

每小时,RITA 导入 Zeek 连接数据,按源/目的地组合开展统计分析,从四个维度评分:周期性、抖动、字节大小一致性与连接持续时间。持续频闪与威胁情报命中单独呈现。

3 基于签名的 IDS 叠加 `Suricata IDS`

Suricata 同时运行,匹配数千条社区与 Emerging Threats 签名。STREAM 与 QUIC 噪声自动过滤。告警通过 MAC 与 IP 与资产清单关联。

4 高性能存储 `ClickHouse · log2ram`

在 NVMe SSD 上的列式时序数据库存储信标评分、连接记录、IDS 告警与主机指标。跨数周数据的查询延迟在毫秒以内;实时日志先写入 RAM 层以延长 SSD 寿命。

5 Web 仪表盘 `Flask · Chart.js · HTTPS`

基于 Flask 的 Web 应用,通过 HTTPS 提供各检测层的实时可见性。十个专用页面覆盖信标、IDS、资产、情报、健康、备份与硬件遥测。

6 告警与每日摘要 `Slack · AWS Lambda · 邮件`

每日 07:00 摘要汇总信标得分最高的主机。实时告警经 AWS Lambda 推送至 Slack,可按类型启用/停用,并按告警设置抑制窗口。仪表盘支持任一告警的测试触发。

检测覆盖

周期性 C2 信标
统计抖动与周期性评分能识别恶意软件的连接,无论其是否经过混淆。

持续单点连接
指向单一目的地的长连接 — 活跃 C2 通道的典型迹象。

Tor 出口节点访问
与已知 Tor 基础设施的连接立即标记 — 可靠的入侵指标。

威胁情报命中
将访问目的地与精选威胁情报源比对 — 已知恶意 IP 与域名。

漏洞利用尝试
Suricata 规则覆盖活跃漏洞利用签名:CVE 载荷、Shellcode、协议滥用。

高熵 DNS 查询
看似随机的子域名 — DGA 与 DNS 隧道的常见特征 — 按 SLD 熵值评分。

异常 DNS 查询量
产生异常高 DNS 查询量的主机 — 这是 C2 探测的常见迹象。

新增与异常设备
局域网中出现新 MAC 时立即触发通知。

告警标准

实时告警

- 高分信标(满分 1.0)
- 持续单点连接流量
- 威胁情报目的地命中
- Tor 出口节点访问
- Suricata P1 局域网规则
- Suricata P1 重复命中
- 服务下线(Zeek / CH / Suricata)
- 磁盘 > 90% 已用
- 局域网新增设备

每日摘要

- 信标得分最高的主机
- Suricata P2 / P3 汇总
- 过去 24 小时新出现的设备
- DNS 高查询量主机
- TLS / DNS 异常摘要
- 误报抑制流量回顾
- 健康与容量概览

自监控的设备

持续健康监控
所依赖的每个服务按计时器检查。故障自动推送 Slack,附诊断信息。

硬件遥测
CPU 温度、风扇转速、内存、磁盘与运行时长。分级散热保持静音。

备份与恢复
三层备份,含整机克隆至 USB SSD。文档化的恢复流程。

加密远程访问
可选 Tailscale 接入实现安全远程支持 — 无入站端口暴露。