思科安全终端调查快照信息

目录

简介

本文档介绍取证快照可以从终端收集的特权信息。

作者：思科软件工程师Pedro Medina。

先决条件

Cisco

- 思科“安全终端”控制台
- 思科“轨道”

要求

- 通过管理员或非管理员用户访问“安全终端”
- 访问思科“轨道”

  注意：如果您的用户为非管理员，您必须通过TAC支持团队请求启用“非管理员调查分析快照”功能。

一般信息

请求调查快照后，信息将以表格式呈现，基于所需的信息，用户可在此说明表中找到任何所需信息：

名称	含义	隐私问题
Autoexec项目	计算机启动时运行的项	无
Bitlocker加密监控	每个已装载驱动器的加密状态	对文件的未加密版本有一定的可视性
DNS缓存表监控	最近搜索的域	最近的浏览器历史记录。
主机文件数据	主机文件中的项目	无
主机上已安装的程序	已安装的应用程序	无

侦听端口	列出打开网络侦听程序的程序	无
加载的模块散列	运行动态链接库(DLL)文件的哈希值	无
加载的模块进程	运行的进程的名称、路径和PID	无
加载的模块与进程	从已加载模块到“进程”表中PID的模块ID映射	无
登录会话	登录用户，包括系统用户	无
映射驱动器	本地和远程装载点、文件系统类型、引导分区信息、加密信息。	无
网络连接 — 进程	将入站和出站网络连接映射到特定PID，并显示启动过程的启动命令行。	可能暴露某些应用（可能是私有应用）络连接。
网络接口	设备上所有物理和虚拟网络接口的列表	无
网络配置文件注册表	计算机连接的网络列表。	可能暴露的WIFI SSID。
操作系统 版本	操作系统的版本	无
Powershell历史记录	设备上运行并存储在系统中的所有Powershell命令的列表。	可能暴露密码、加密API密钥和编码到脚的其他敏感数据。
预回迁目录	内存管理功能 — 操作系统将尝试预加载频繁的可执行文件以节省启动时间。	用户习惯的暴露。
最近的文件数据	最近使用/访问的文件	暴露用户习惯和私有文件名。
运行文件散列	名称、路径、命令行、PID，所有运行的可执行文件的所有者。	无
运行服务监控	所有运行服务的名称、服务类型、PID和启动类型	无
计划任务	设置为在系统上定期运行的所有自动任务的列表	无
共享的资源	在系统中打开共享	无
启动项目	在计算机启动时运行的项目 — 与autoexec不同，这些项目存储在注册表项中	无
系统网络状态监控	网络统计	无
临时目录文件数据	进程创建的临时文件	用户浏览历史记录可能泄漏。
受信任的根证书	受信任的根证书存储区数据转储	无

UBSTOR注册表项	插入USB设备的历史记录	显示设备序列号。
用户组	计算机上的本地组	无
UserAssist监控	显示最近执行的文件	可能暴露隐藏行为，例如运行加密或擦具。
用户	设备上的本地用户	无
用户 — 已登录	当前登录设备的本地用户	无
WMI事件过滤器监控	监视特定项目的事件日志	无
Windows AV产品监控	系统上安装了哪种防病毒软件（如果有）	无
Windows BAM条目监控	提供文件执行证明	可能暴露行为
Windows环境变量	显示路径信息、系统变量等	无
Windows修补程序	所有已安装的修补程序列表	无
Windows NT域搜索	计算机可对其进行身份验证的域列表	无
Windows ShellBags监控	提供有关用户访问文件夹和查看文件夹首选项等的信息。	用户习惯的暴露。
Windows ShimCache监控	跟踪与可执行文件的兼容性	用户行为的暴露。
Chrome扩展监控	列出Chrome扩展	用户行为的暴露。
Windows Office MRU	列出每个Office应用程序的最新使用文件	敏感文件名和用户行为的暴露