

反编译计算

ssdeep检测

文件黑白名单计算

Yara检测(规则命中)

机器学习检测(对应不同类不同尝试)

文件黑白名单计算

略,待研究

MD5 Fuzzy Hash SHA1 文件头 文件尾 文件内重合指数 文件内信息熵 文件内容有意义程度布尔值 Yara黑名单命中 布尔值 Yara 白名单命中 布尔值 SSdeep黑名单命中 布尔值 时间戳标记 文件名称 大小 size: kb,mb 占用空间 storage: kb.mb 类型 type: bin,txt,doc,registry,thread,network 后缀 suffix: txt,dll,exe 路径 filepath: C:/home/ 所属用户 文件权限: write,read,exeute 用户权限 rights: admin,user,guest 所属用户组 所属用户组权限 鉴别结果 检测方法 基本文件操作

时间戳计算

用户及用户组归属和权限判断

注册表

文件名

文件路径

文件类型

MD5计算

SHA1计算

杀软日志: 布尔值

系统日志: 布尔值

用户命令行历史

Yara检测(匹配)

文件黑白名单计算

时间戳标记

日志信息

人工逻辑

时间戳计算

注册表日志: 布尔值

机器学习检测(文本分类)

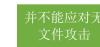
文件内重合指数

文件头文件尾读取

文件内信息熵

Fuzzy Hash计算

关键注册表项 鉴别结果 yara检测(匹配) 人工逻辑



util文件

时间戳计算 进程名和进程ID读取 内存状态读取计算 CPU状态读取计算 磁盘读写状态计算 进程文件溯源查找 危险内存区判断 权限提升判断及迹象判断 用户及用户组归属和权限判断 IP黑白名单计算 文件黑白名单计算 是去向所有网络信息中 查到,还是单独由进程 DGA僵尸家族识别 端口端口服务一致性检验 定位 进程网络信息计算

进程ID 进程名 父进程ID 父进程名 子进程ID 子进程名 时间戳标记 所属用户 所属用户权限 所属用户组 所属用户组权限 权限提升: 布尔值 文件溯源: 布尔值 文件溯源信息 内存起始地址 内存结束地址 危险内存区: 布尔 网络行为: 布尔 网络行为信息 I/O行为: 布尔 I/O行为信息 内存前后占比 CPU前后占比 鉴别结果 检测方法 时间戳计算 CPU前后占比计算(先由通用函数计算) 内存前后占比计算(由通用函数计算) 进程文件溯源计算 进程网络信息计算 危险内存区判断 权限提升判断

用户及用户组归属和权限判断

进程名和进程ID读取 综合计算???

DGA计算

端口端口服务一致性检验

协议名称 上传速度 下载速度 时间戳标记 源域名或IP 目的域名或IP DNS服务器 跃迁节点 端口 端口服务 10秒内携带数据摘要 代理行为 代理行为信息 整体网络上传下载信息 IP黑白名单计算 代理行为判断