SACI: Solução Automatizada para Análise Comportamental de Código Infeccioso em SO MS Windows Modernos

Bernardo P. Tomasi, Davi C. Ribeiro, Pedro Friedrich, Ruibin Mei, Yago Furuta, Jorge Correia, André Grégio

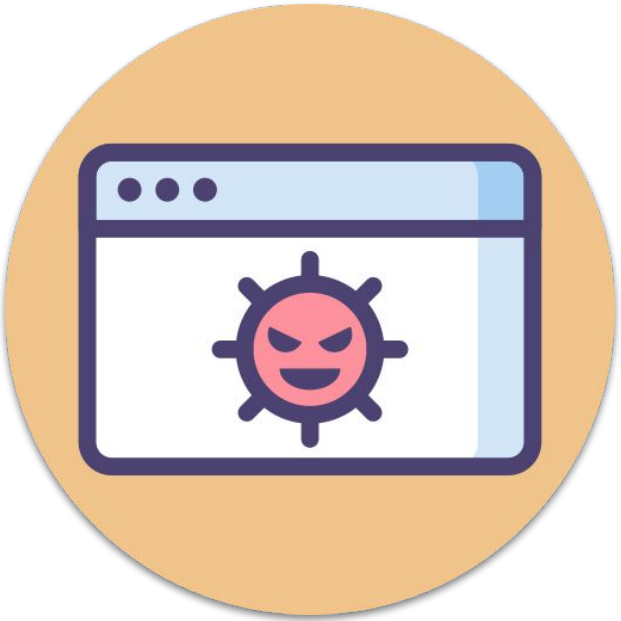
Universidade Federal do Paraná

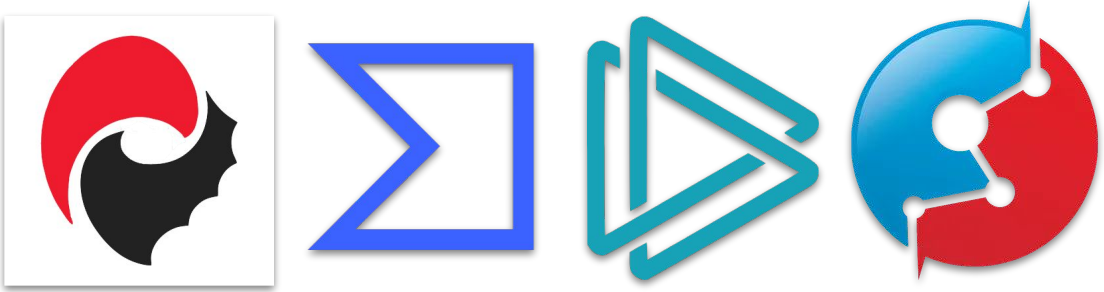
UFPR
UNIVERSIDADE FEDERAL DO PARANÁ

SECRET

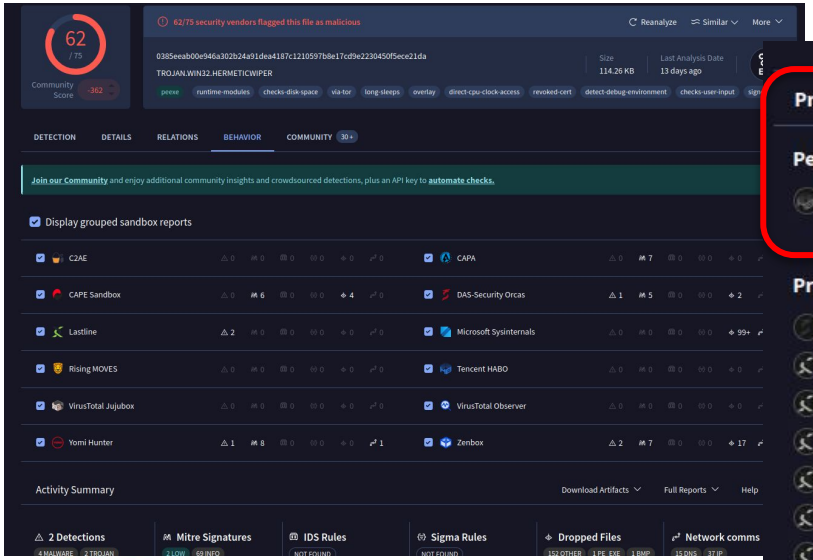
./C3SL
UFPR

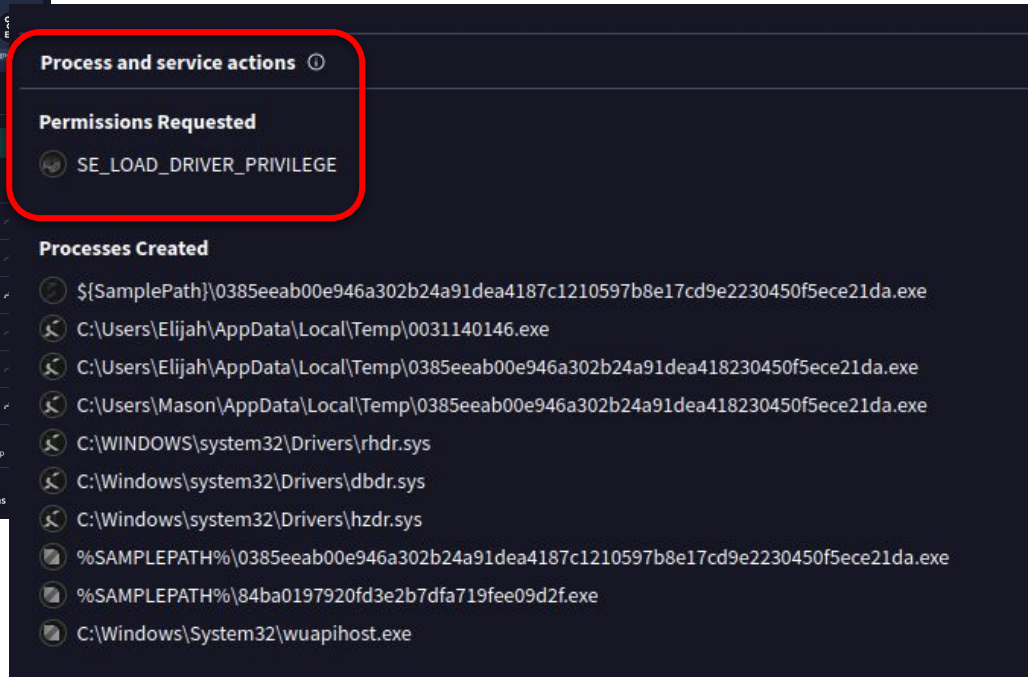
Motivação





Problema(s)



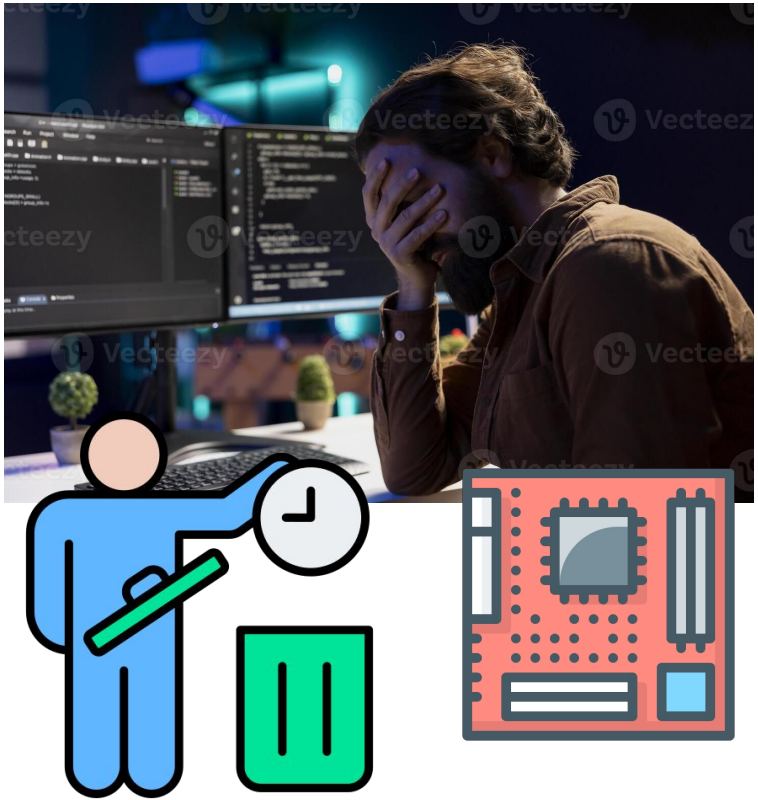


SIGMA

yara

Superficialidade

Problema(s)

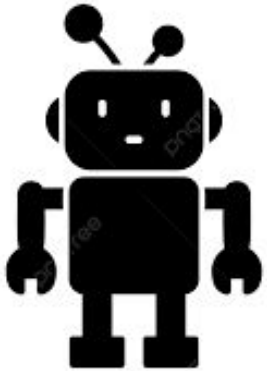


Setup trabalhoso e demorado

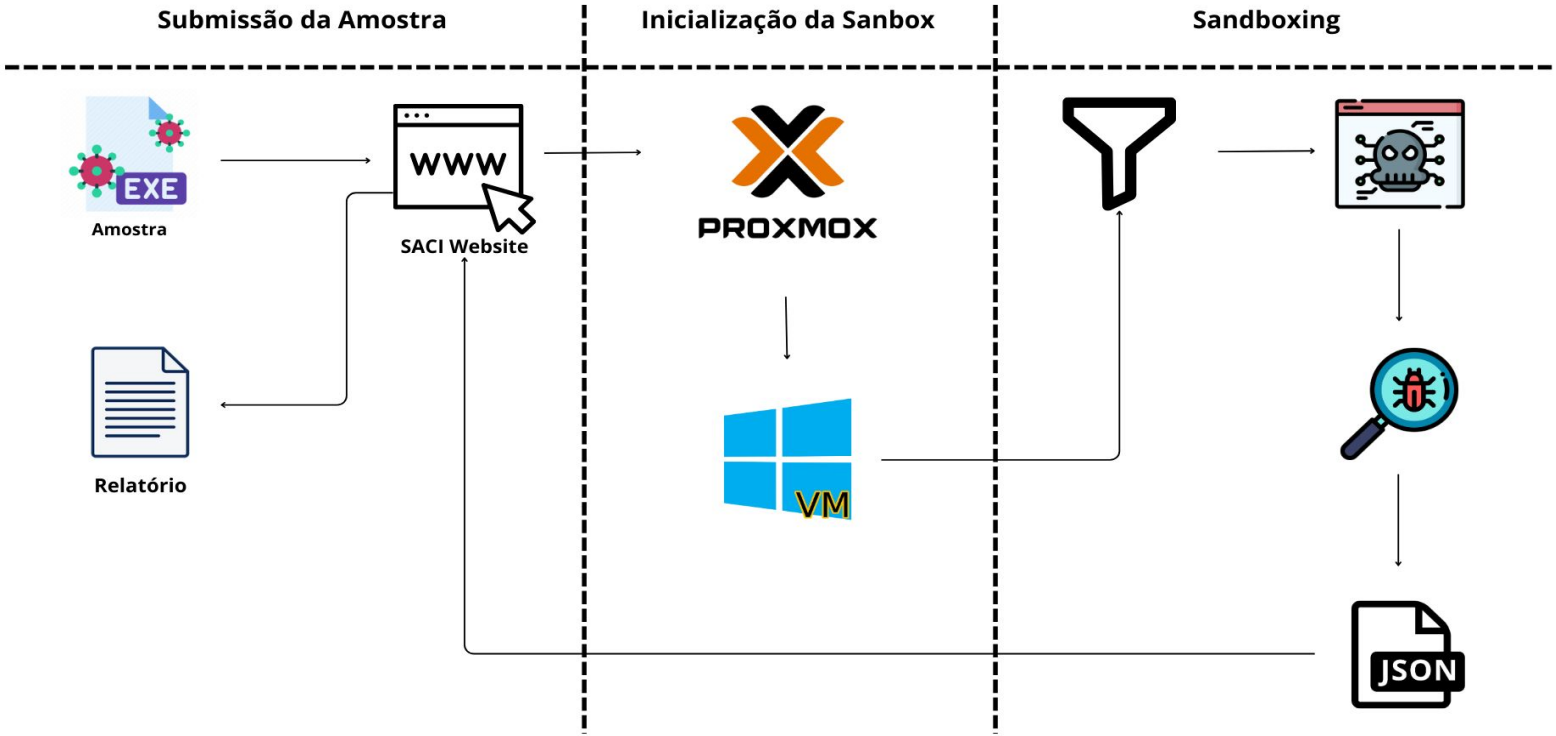
Desafio(s)

Encontrar um meio termo entre a profundidade da análise e automação

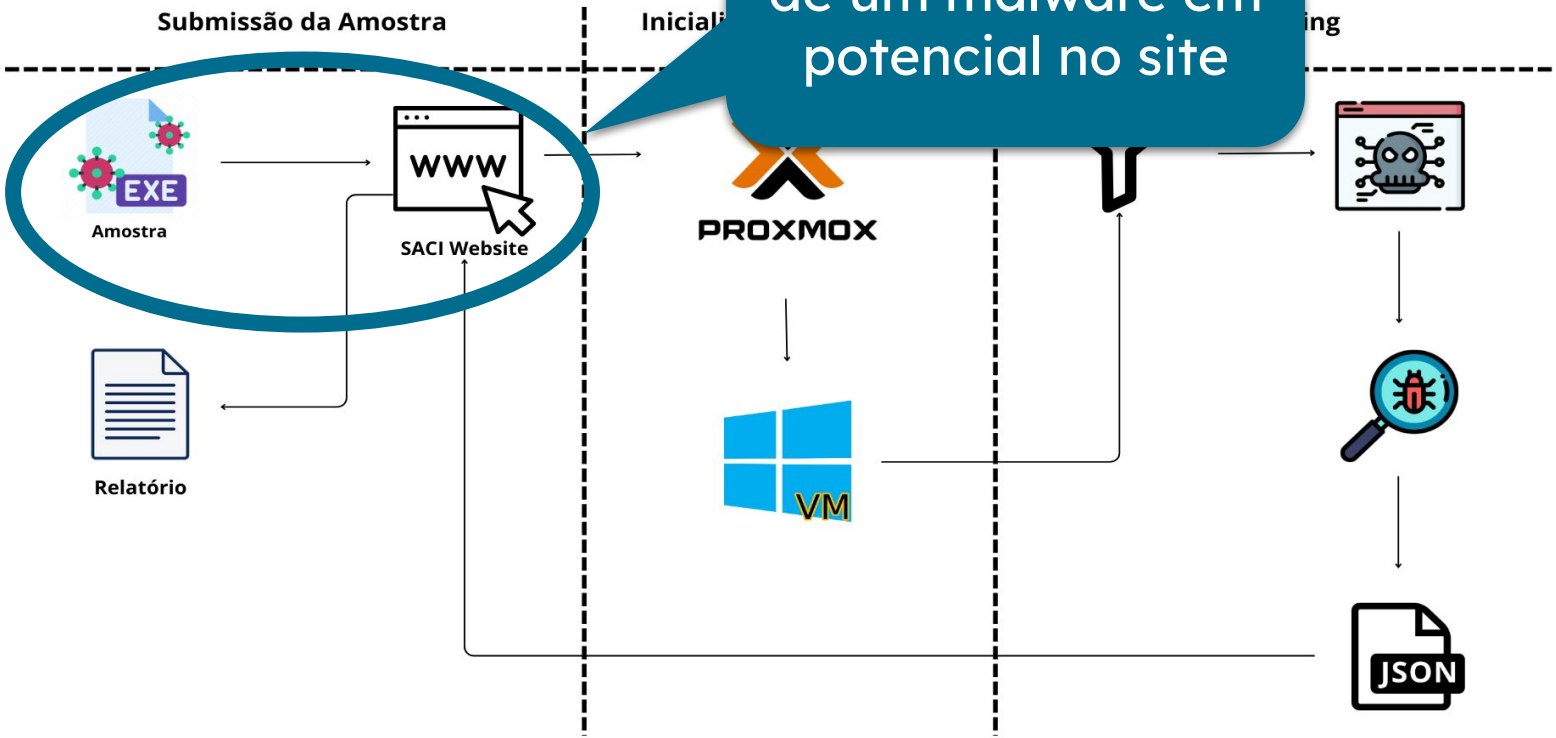
VS



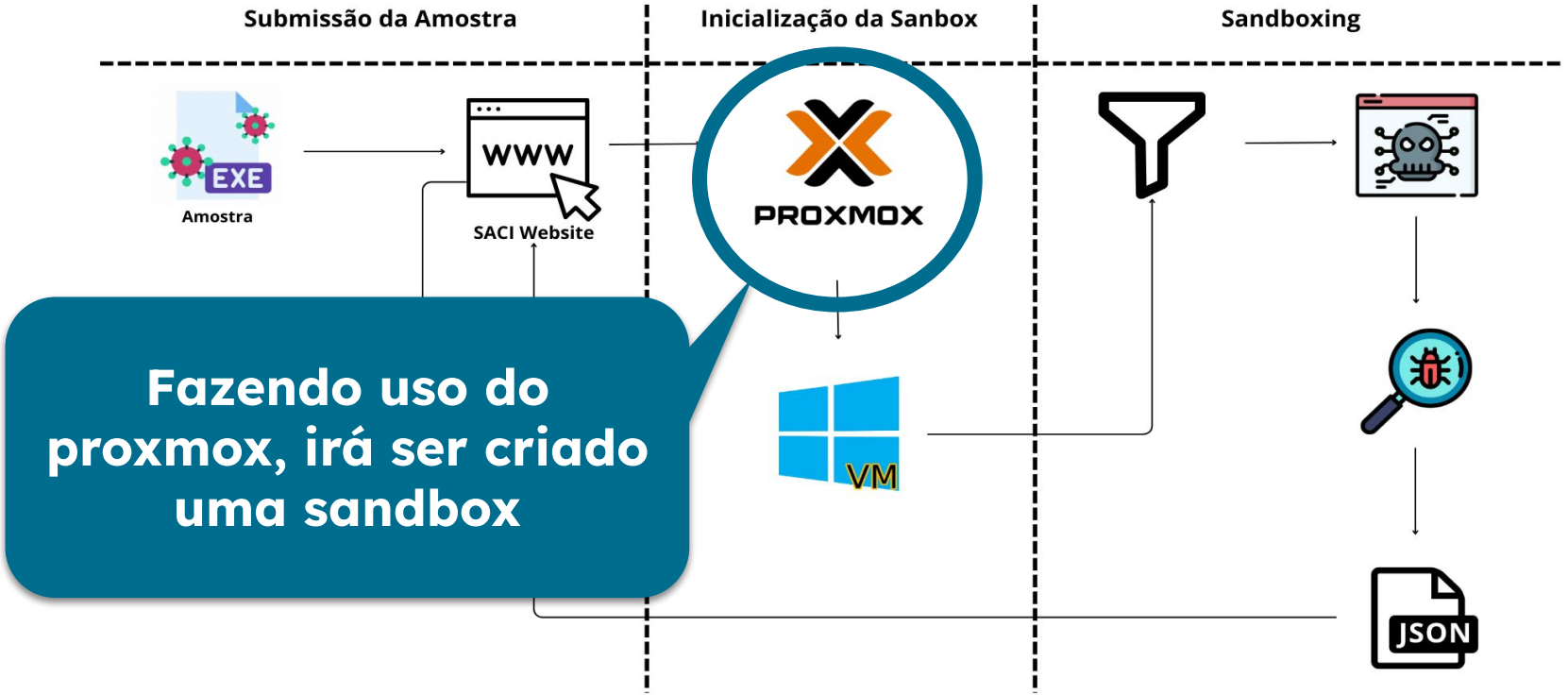
Solução Proposta



Solução Proposta



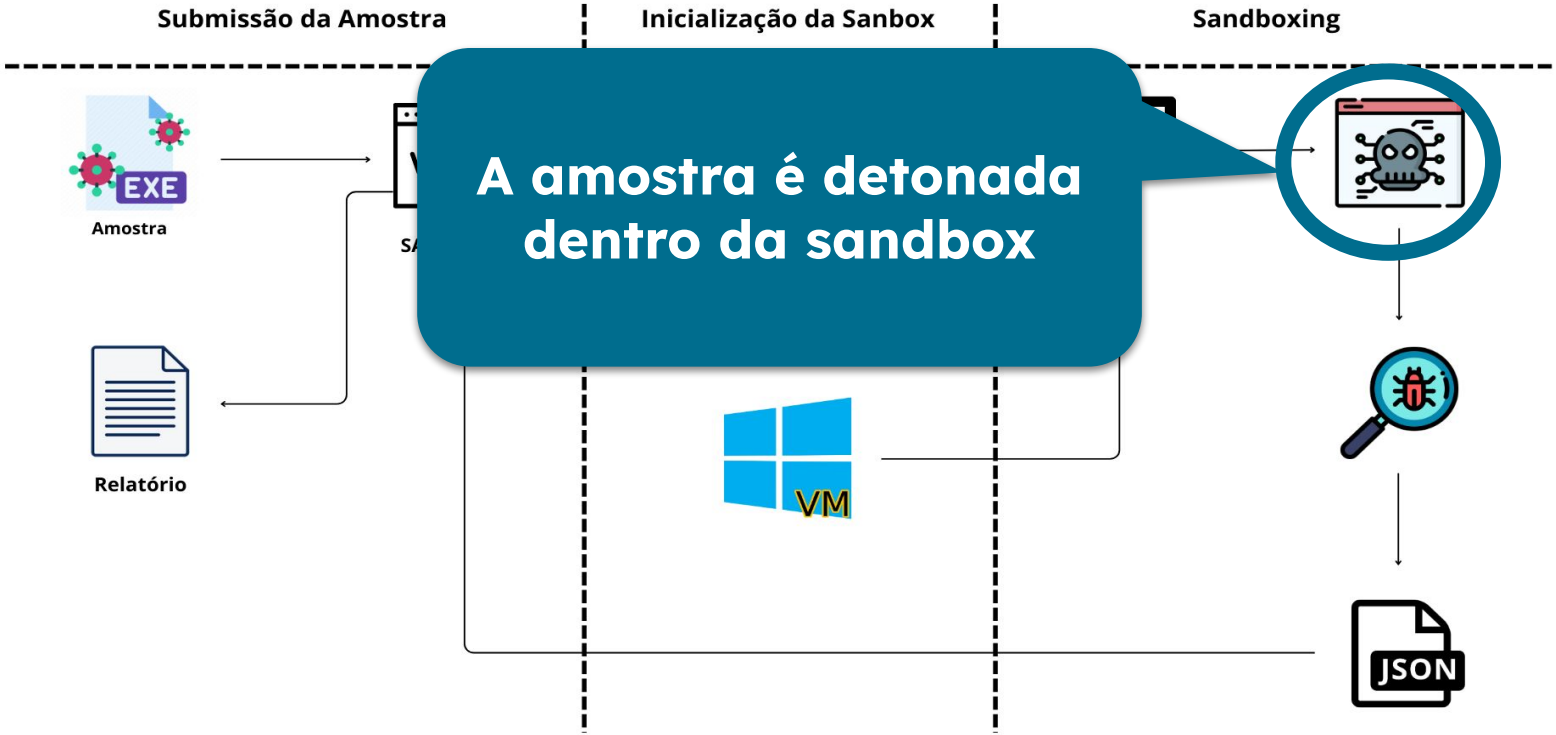
Solução Proposta



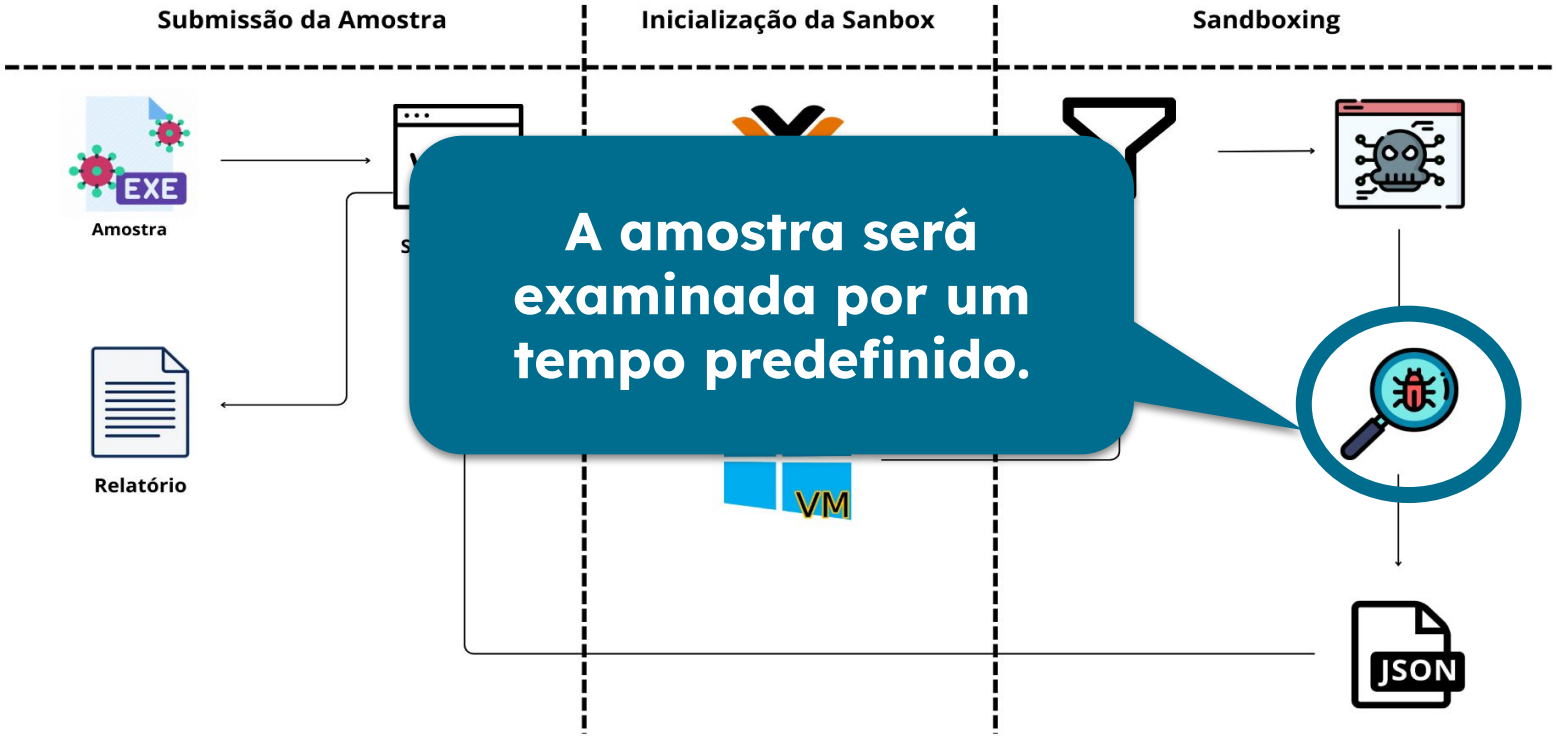
Solução Proposta

Solução Proposta

Solução Proposta



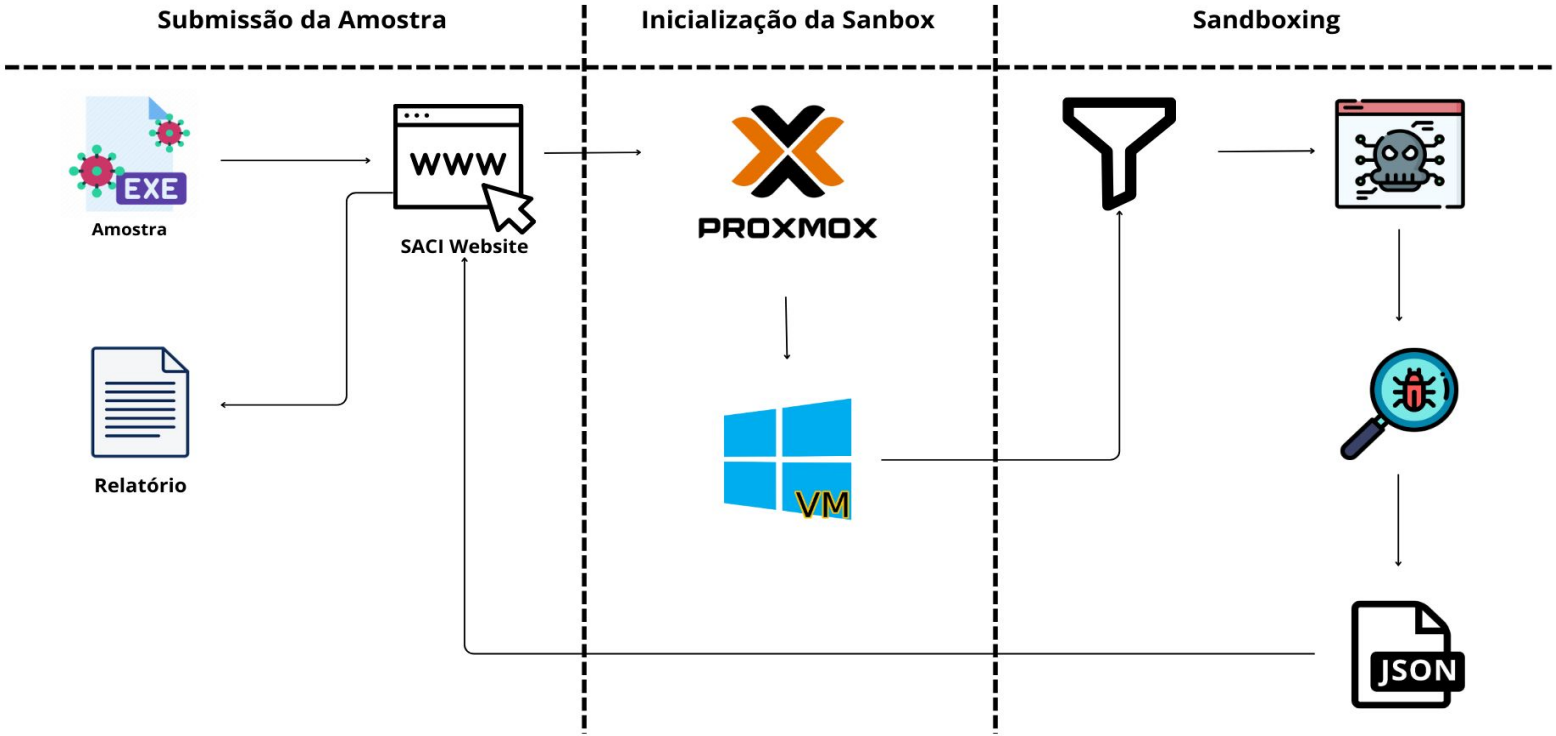
Solução Proposta



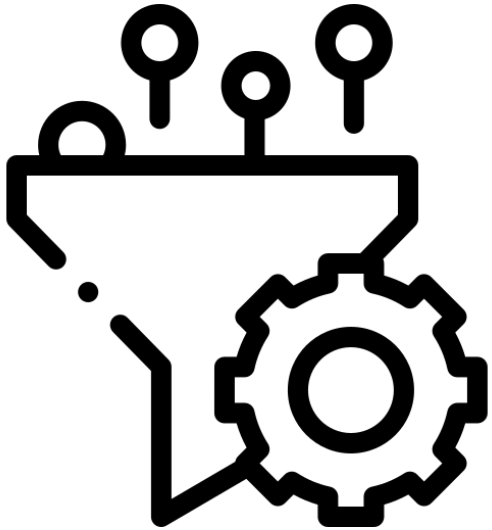
Solução Proposta

Solução Proposta

Solução Proposta



Filtragem



Driver de Filtragem:

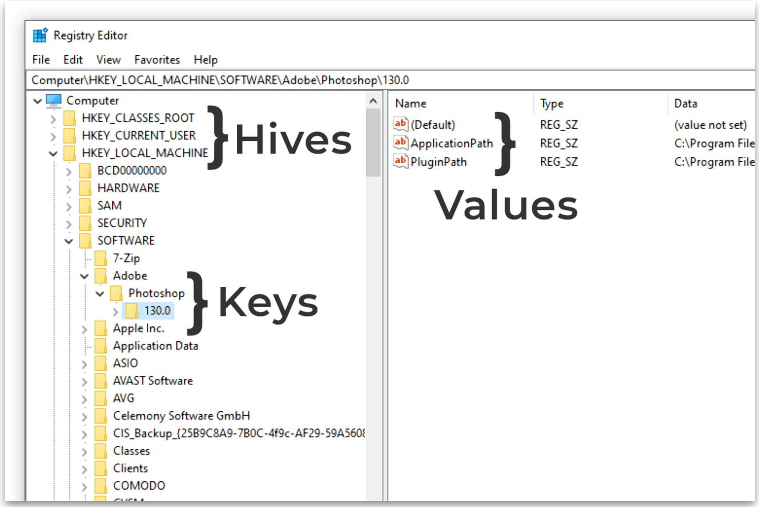
- **Permite acesso a nível de kernel a todos os acontecimentos do sistema**

- **Mais estável e maior suporte comparado a uma engine hooks**

Filtra:

- **Eventos no Sistemas de Arquivos**
- **Ações no Registros**
- **Carregamento de Imagem**
- **Criação e Deleção de Processos**

Filtragem



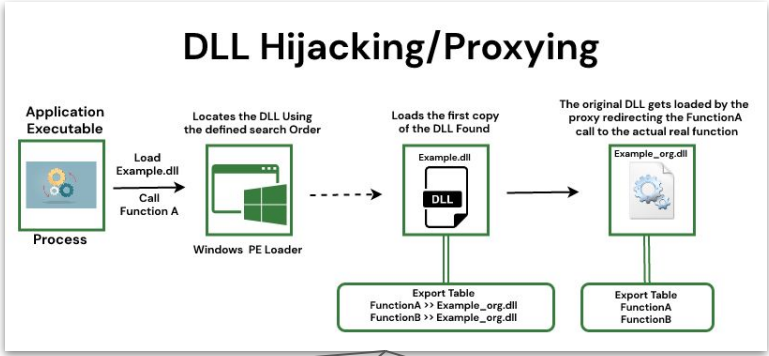

```
{
  "date":"4/9/2024",
  "time":"11:31:19:143",
  "info type":"INFO_REG",
  "registry operation":"RegNtSetValueKey",

"name":"\\REGISTRY\\MACHINE\\SOFTWARE\\WOW6432Node\\Microsoft\\Tracing\\malware_RASAPI32",
  "data type":"REG_DWORD",
  "data":"0 0 0 0 "
}
```


Registros

Filtragem


```
{
  "date":"4/9/2024",
  "time":"11:31:17:815",
  "info type":"INFO_LOAD",
  "pid":"2000",
  "full image
name":"\\Device\\HarddiskVolume3\\Windows\\System32\\ntdll.dll",
  "file name":"\\Windows\\System32\\ntdll.dll"
}
```

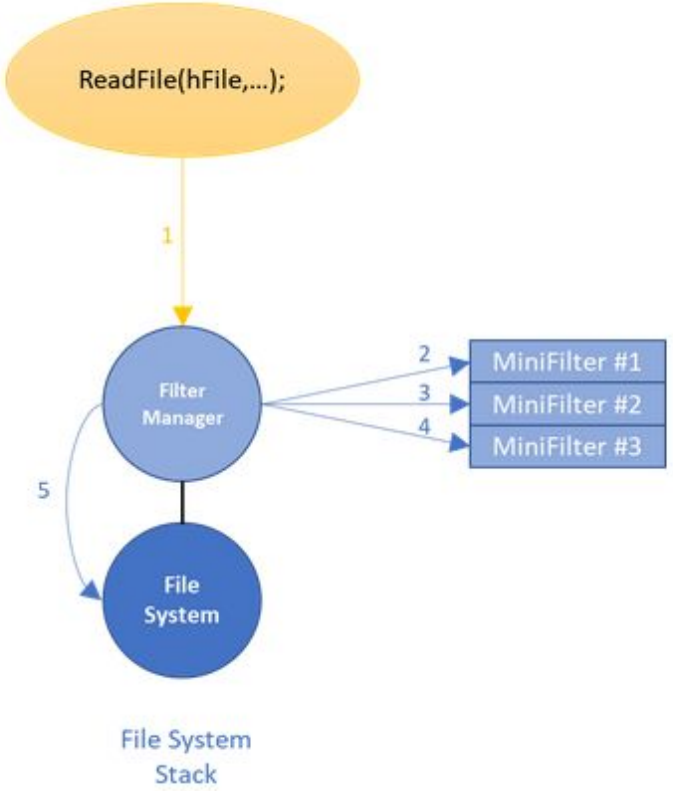
Injection

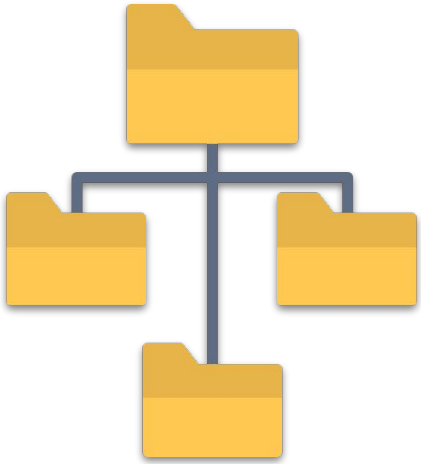
Side-loading

Spoofing

Carregamento de imagens

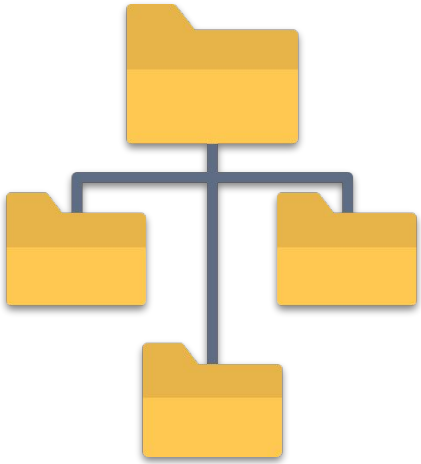
Filtragem





Evento de sistema de arquivos

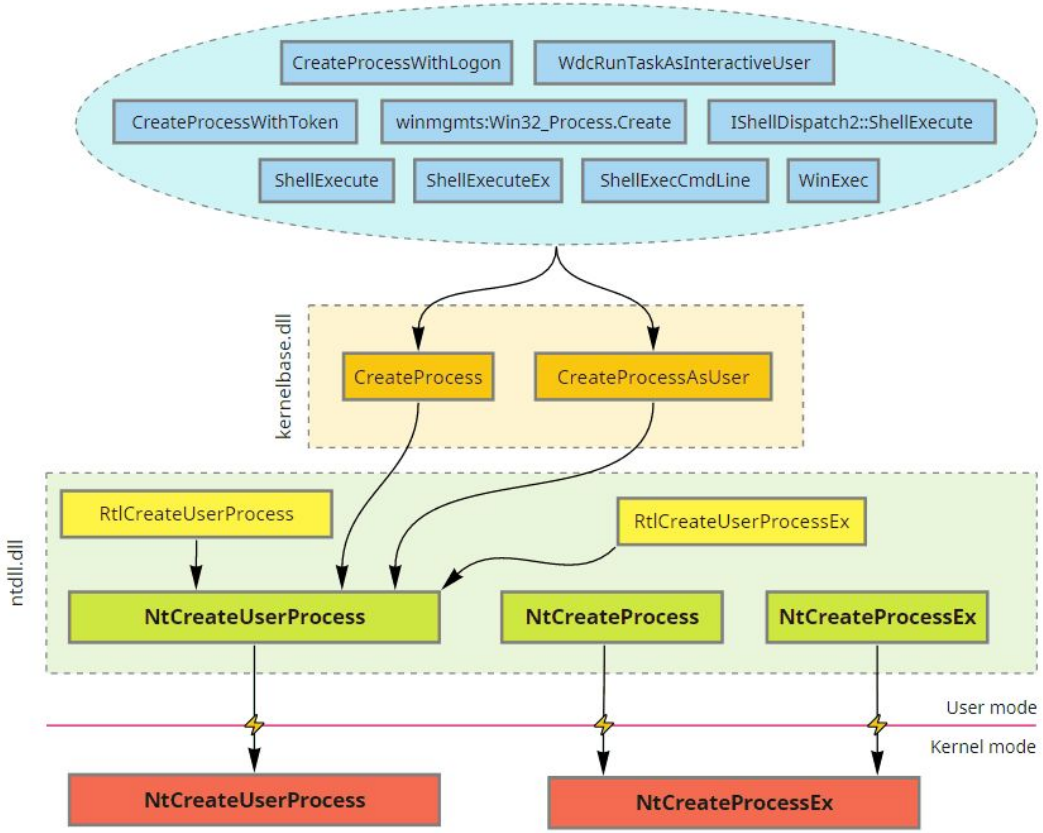
Filtragem



Log


```
{
  "date": "5/9/2024",
  "time": "10:25:28:537",
  "mjFunc": "IRP_MJ_READ",
  "pid": "7584",
  "sid": "1",
  "token type": "primary token",
  "privileges": [
    {"SeIncreaseQuotaPrivilege": "Disabled"},
    {"SeSecurityPrivilege": "Disabled"},
    {"SeTakeOwnershipPrivilege": "Disabled"},
    {"SeLoadDriverPrivilege": "Disabled"},
    {"SeSystemProfilePrivilege": "Disabled"},
    {"SeSystemtimePrivilege": "Disabled"},
    {"SeProfileSingleProcessPrivilege": "Disabled"},
    {"SeIncreaseBasePriorityPrivilege": "Disabled"},
    {"SeCreatePagefilePrivilege": "Disabled"},
    {"SeBackupPrivilege": "Disabled"},
    {"SeRestorePrivilege": "Disabled"},
    {"SeShutdownPrivilege": "Disabled"},
    {"SeDebugPrivilege": "Disabled"},
    {"SeSystemEnvironmentPrivilege": "Disabled"},
    {"SeChangeNotifyPrivilege": "Enabled"},
    {"SeRemoteShutdownPrivilege": "Disabled"},
    {"SeUndockPrivilege": "Disabled"},
    {"SeManageVolumePrivilege": "Disabled"},
    {"SeImpersonatePrivilege": "Enabled"},
    {"SeCreateGlobalPrivilege": "Enabled"},
    {"SeIncreaseWorkingSetPrivilege": "Disabled"},
    {"SeTimeZonePrivilege": "Disabled"},
    {"SeCreateSymbolicLinkPrivilege": "Disabled"},
    {"SeDelegateSessionUserImpersonatePrivilege": "Disabled"}
  ],
  "elevation status": "1265585296",
  "image name": "\Device\HarddiskVolume3\Users\administrator\amaterasu\malware.exe,
  "path": "\Device\HarddiskVolume3\Windows\Prefetch\MALWARE.EXE-8EB74B73.pf",
  "fileName": "MALWARE.EXE-8EB74B73.pf"
}
```

Filtragem



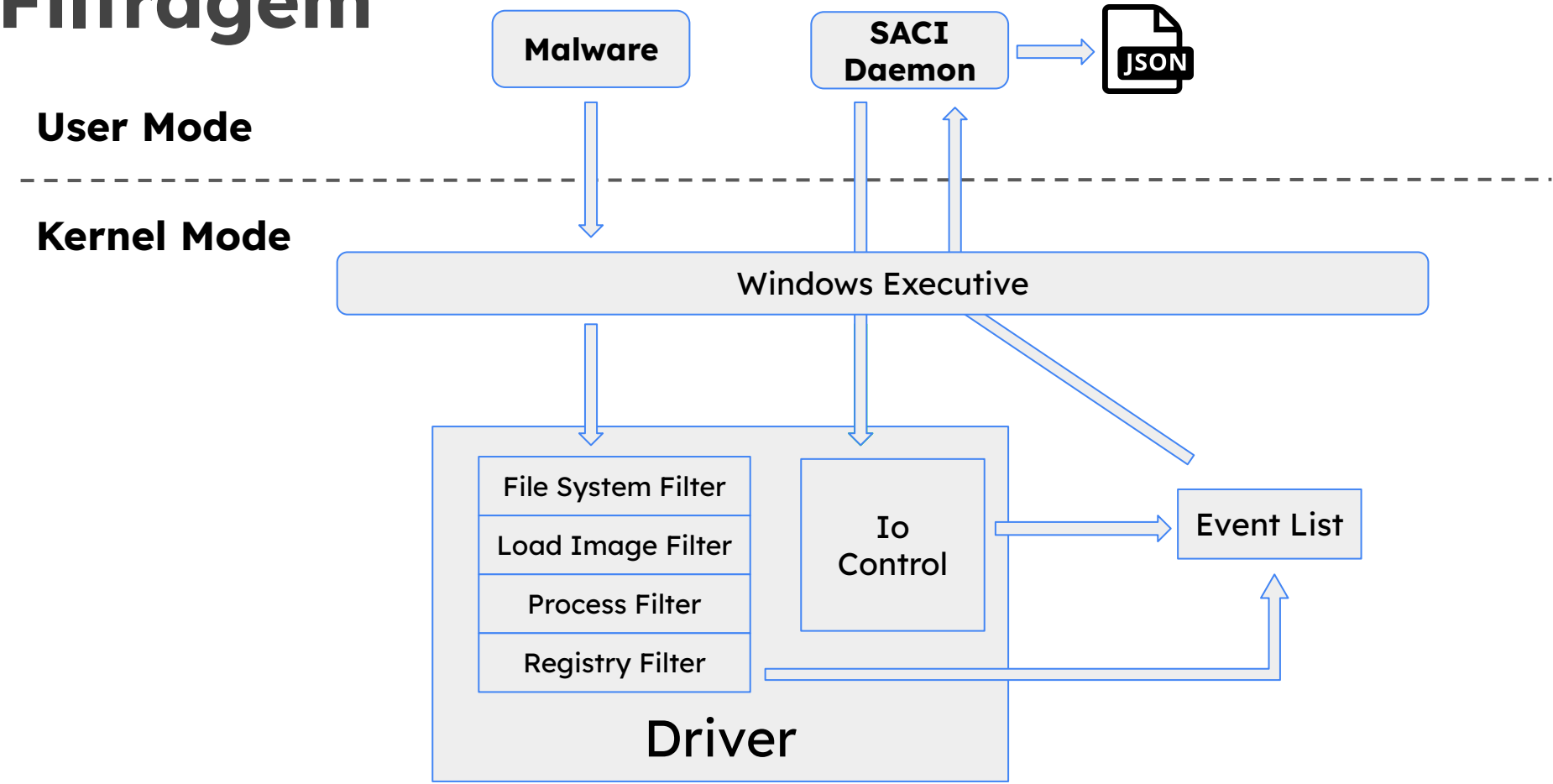
Criação de Processos

Filtragem

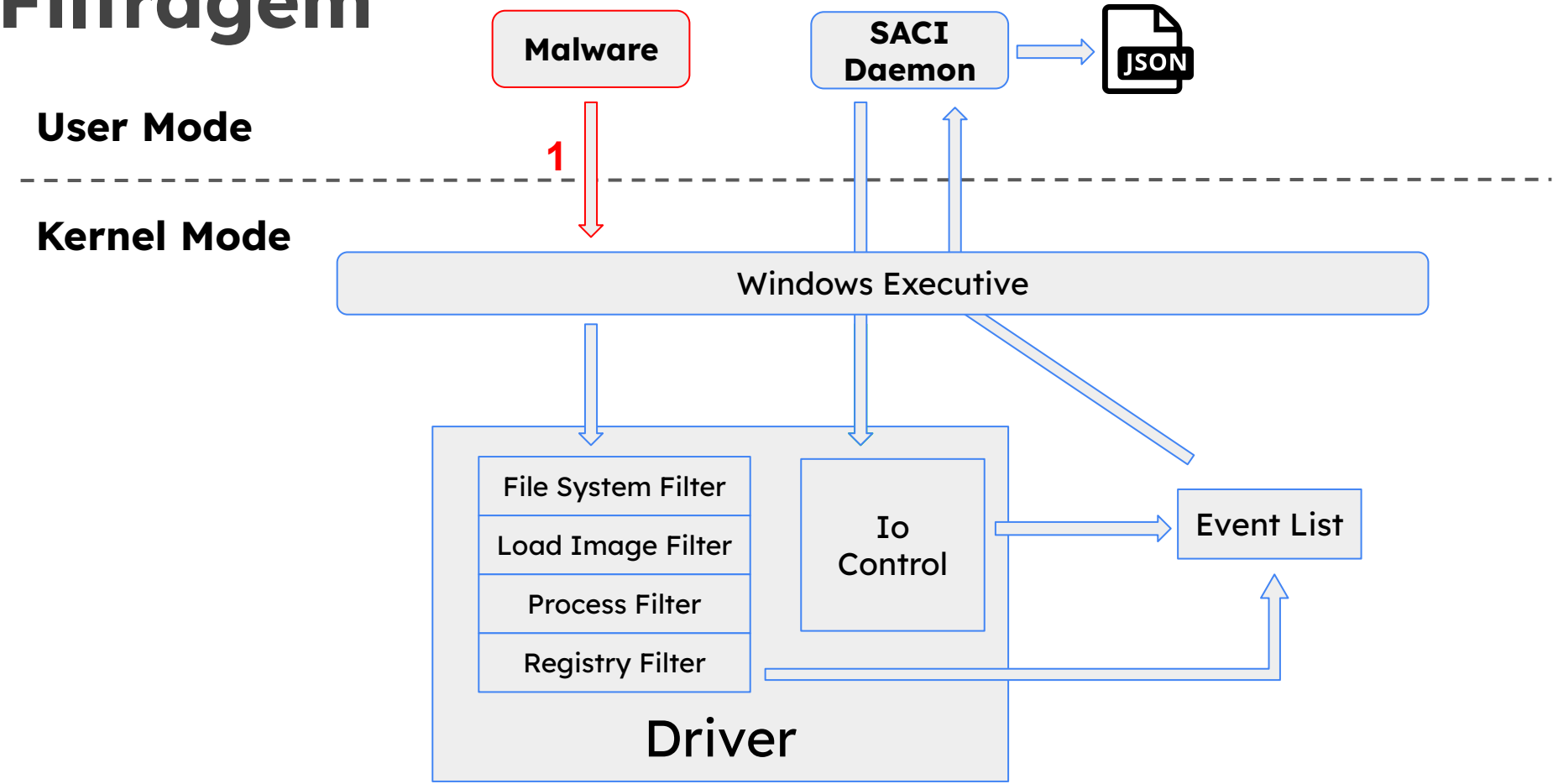
Log


```
{
  "date": "5/9/2024",
  "time": "10:25:28:537",
  "infotype": "INFO_PROC",
  "ppid": "7584",
  "pid": "6860",
  "operation": "create",
  "token type": "primary token",
  "privileges": [
    {"SeIncreaseQuotaPrivilege": "Disabled"},
    {"SeSecurityPrivilege": "Disabled"},
    {"SeTakeOwnershipPrivilege": "Disabled"},
    {"SeLoadDriverPrivilege": "Disabled"},
    {"SeSystemProfilePrivilege": "Disabled"},
    {"SeSystemtimePrivilege": "Disabled"},
    {"SeProfileSingleProcessPrivilege": "Disabled"},
    {"SeIncreaseBasePriorityPrivilege": "Disabled"},
    {"SeCreatePagefilePrivilege": "Disabled"},
    {"SeBackupPrivilege": "Disabled"},
    {"SeRestorePrivilege": "Disabled"},
    {"SeShutdownPrivilege": "Disabled"},
    {"SeDebugPrivilege": "Disabled"},
    {"SeSystemEnvironmentPrivilege": "Disabled"},
    {"SeChangeNotifyPrivilege": "Enabled"},
    {"SeRemoteShutdownPrivilege": "Disabled"},
    {"SeUndockPrivilege": "Disabled"},
    {"SeManageVolumePrivilege": "Disabled"},
    {"SeImpersonatePrivilege": "Enabled"},
    {"SeCreateGlobalPrivilege": "Enabled"},
    {"SeIncreaseWorkingSetPrivilege": "Disabled"},
    {"SeTimeZonePrivilege": "Disabled"},
    {"SeCreateSymbolicLinkPrivilege": "Disabled"},
    {"SeDelegateSessionUserImpersonatePrivilege":
"Disabled"}
  ]
}
```

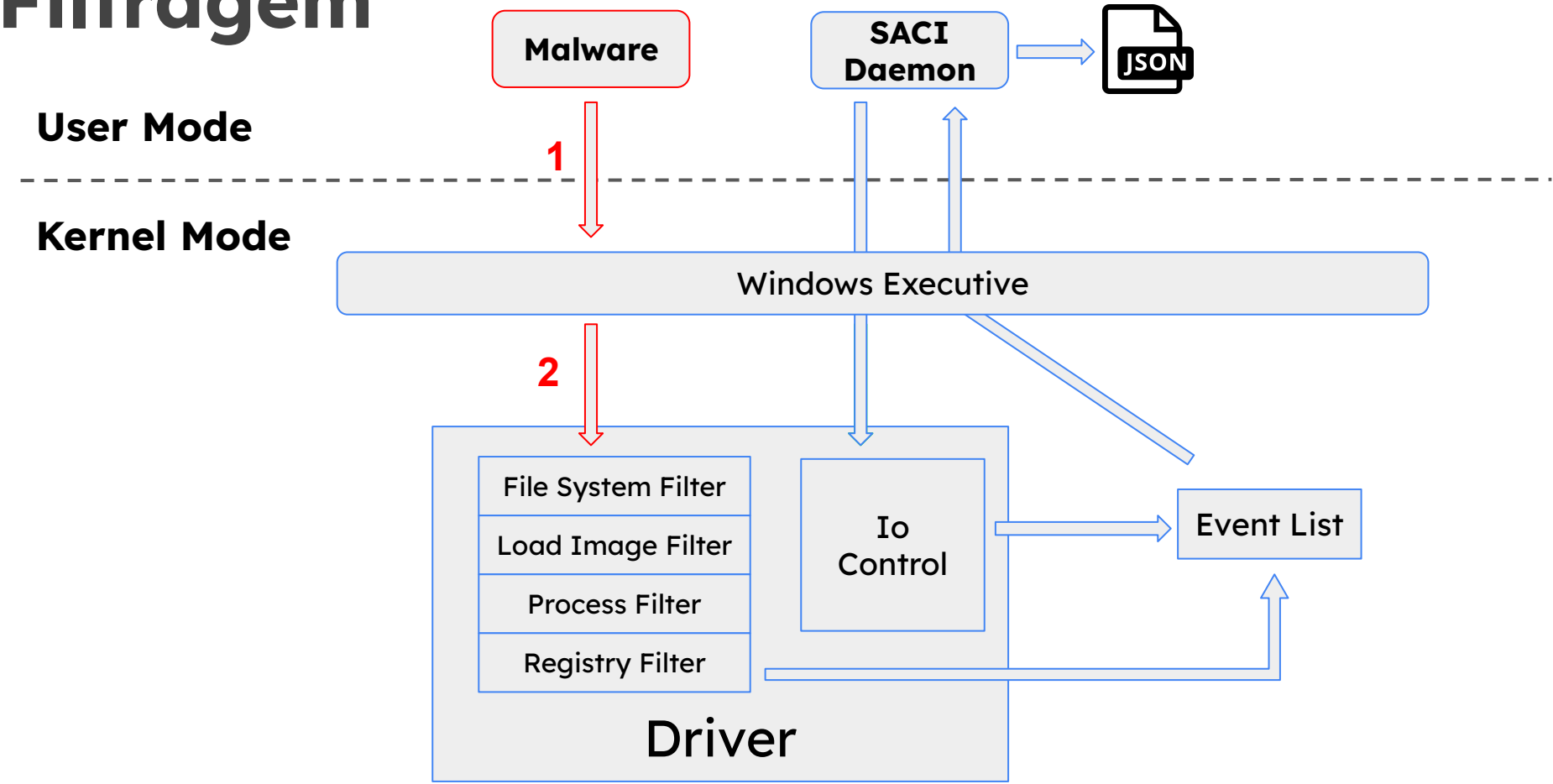
Filtragem


Malware
SACI Daemon
JSON
User Mode
Kernel Mode
Windows Executive
File System Filter
Load Image Filter
Process Filter
Registry Filter
Io Control
Event List
Driver

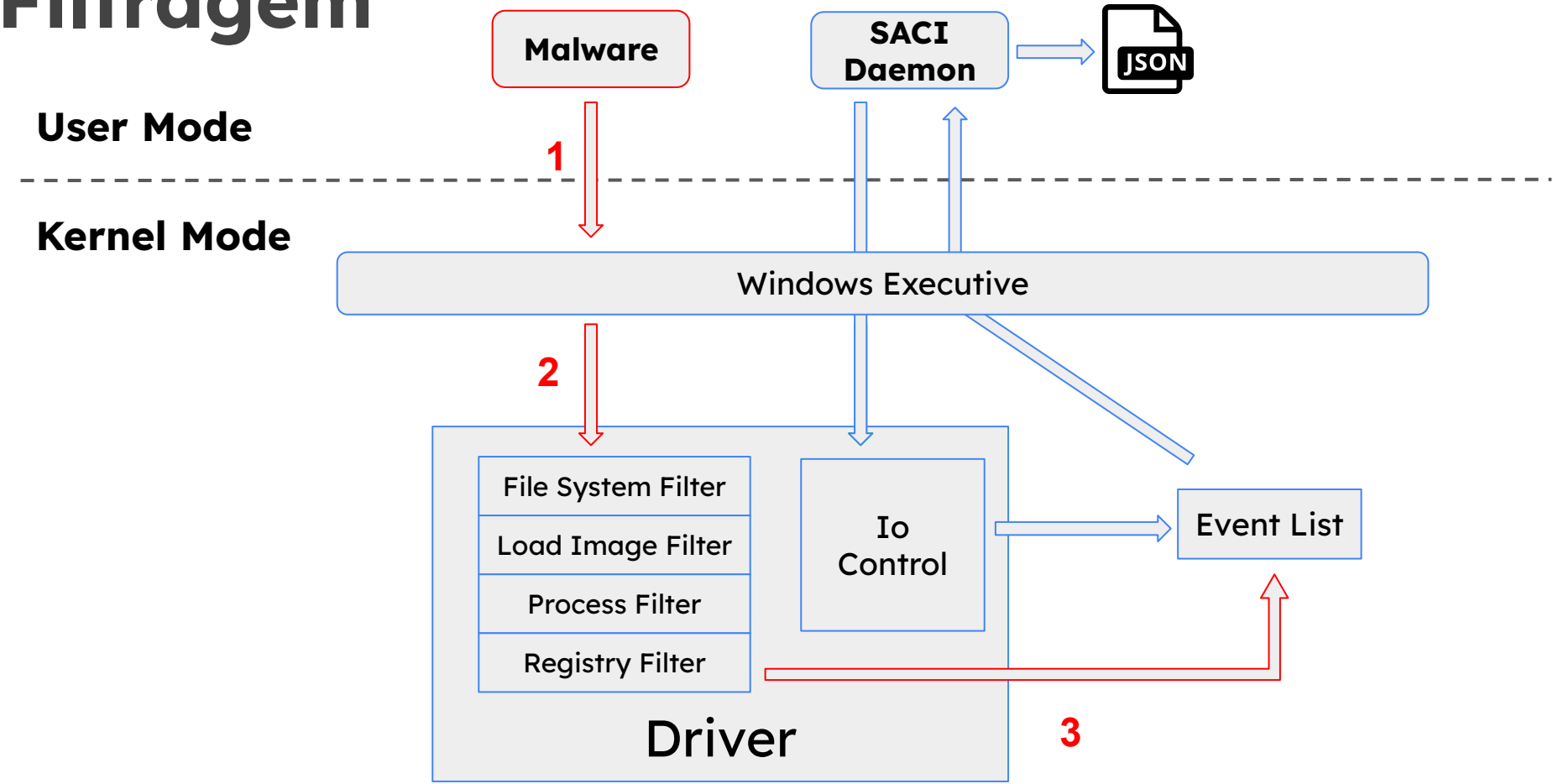
Filtragem


Malware
SACI Daemon
JSON
User Mode
1
Kernel Mode
Windows Executive
File System Filter
Load Image Filter
Process Filter
Registry Filter
Io Control
Event List
Driver

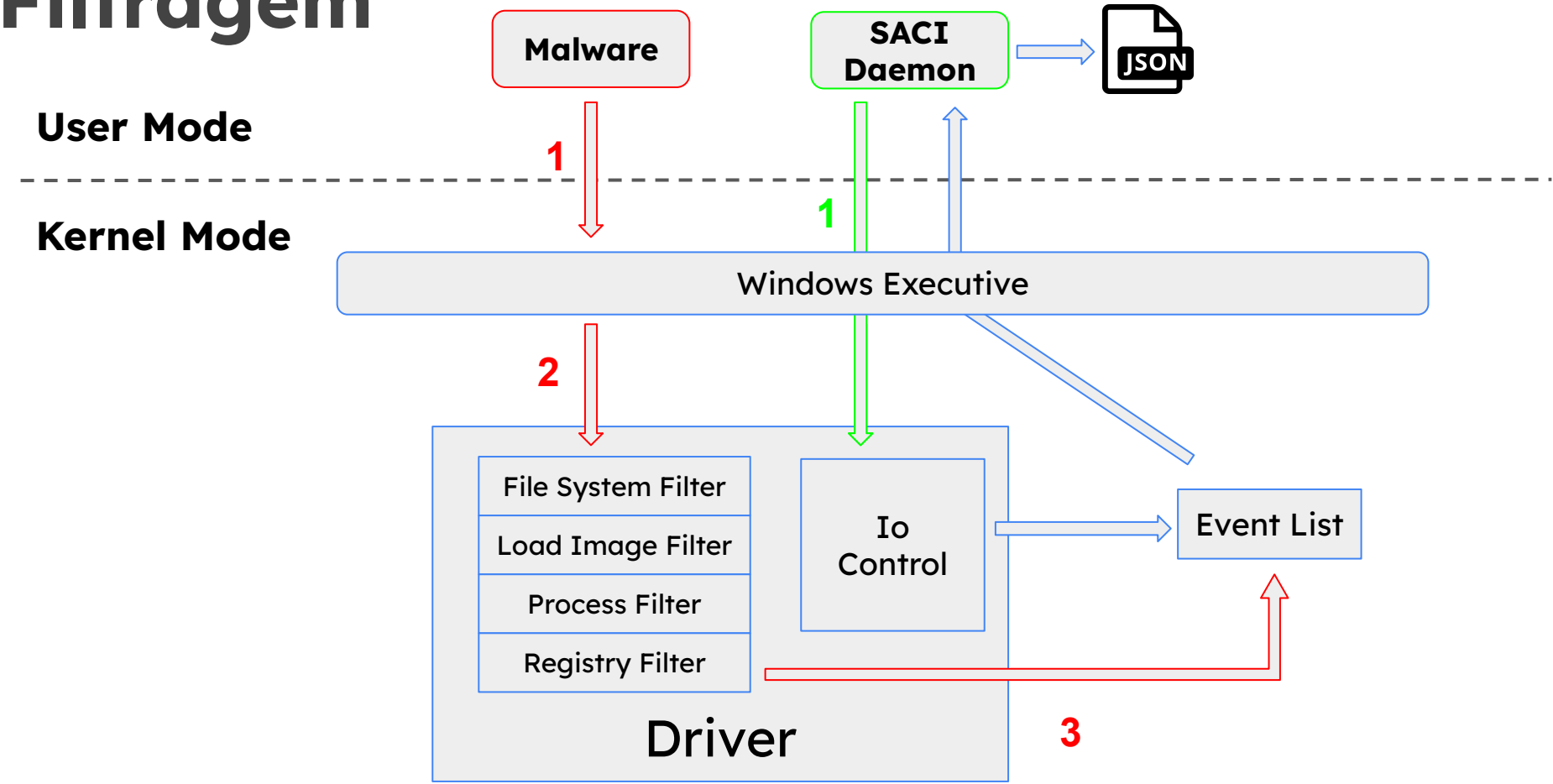
Filtragem


Malware
SACI Daemon
JSON
User Mode
1
Kernel Mode
Windows Executive
2
File System Filter
Load Image Filter
Process Filter
Registry Filter
Io Control
Event List
Driver

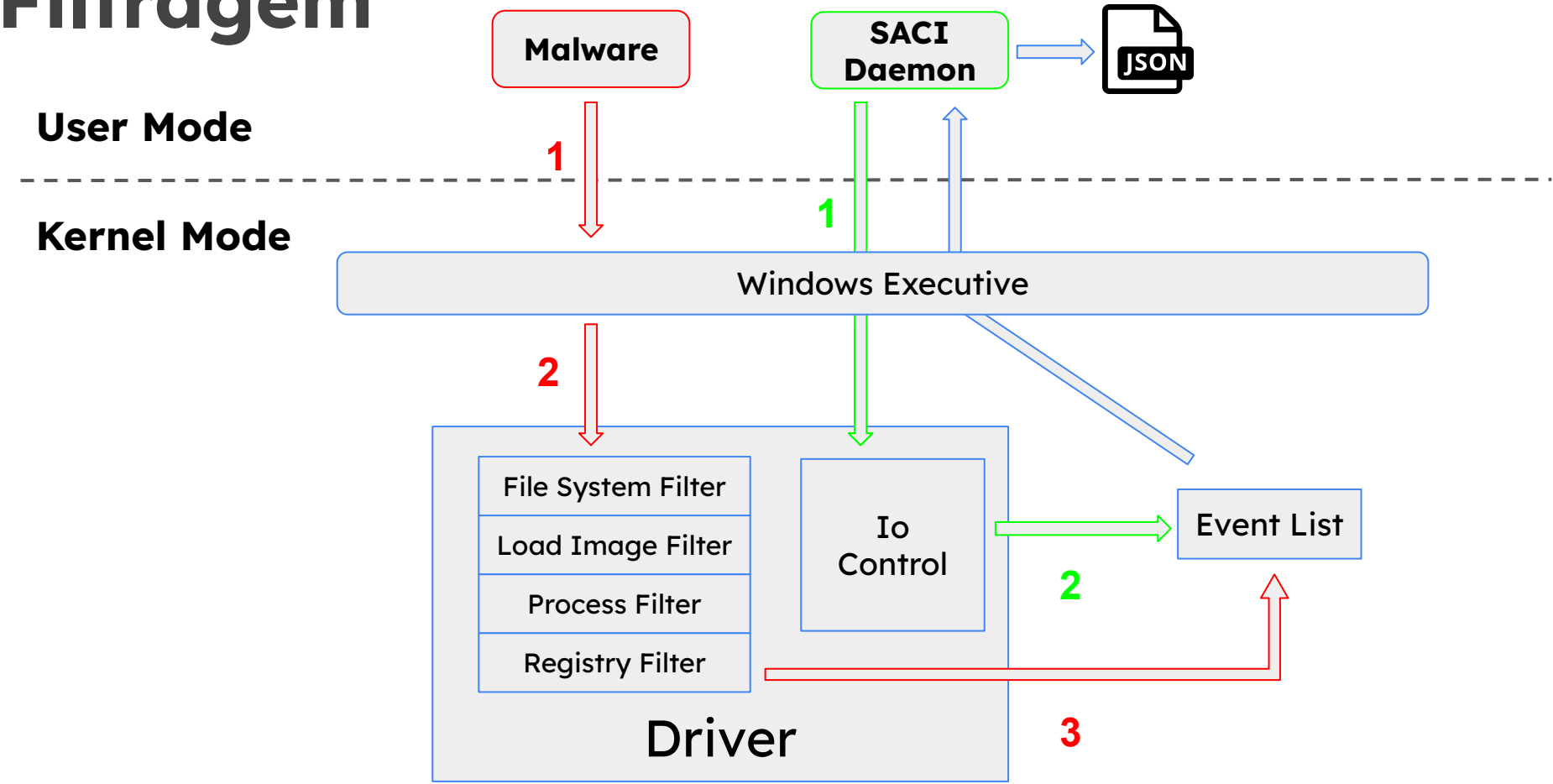
Filtragem


Malware
SACI Daemon
JSON
User Mode
1
Kernel Mode
Windows Executive
2
File System Filter
Load Image Filter
Process Filter
Registry Filter
Io Control
Event List
Driver
3

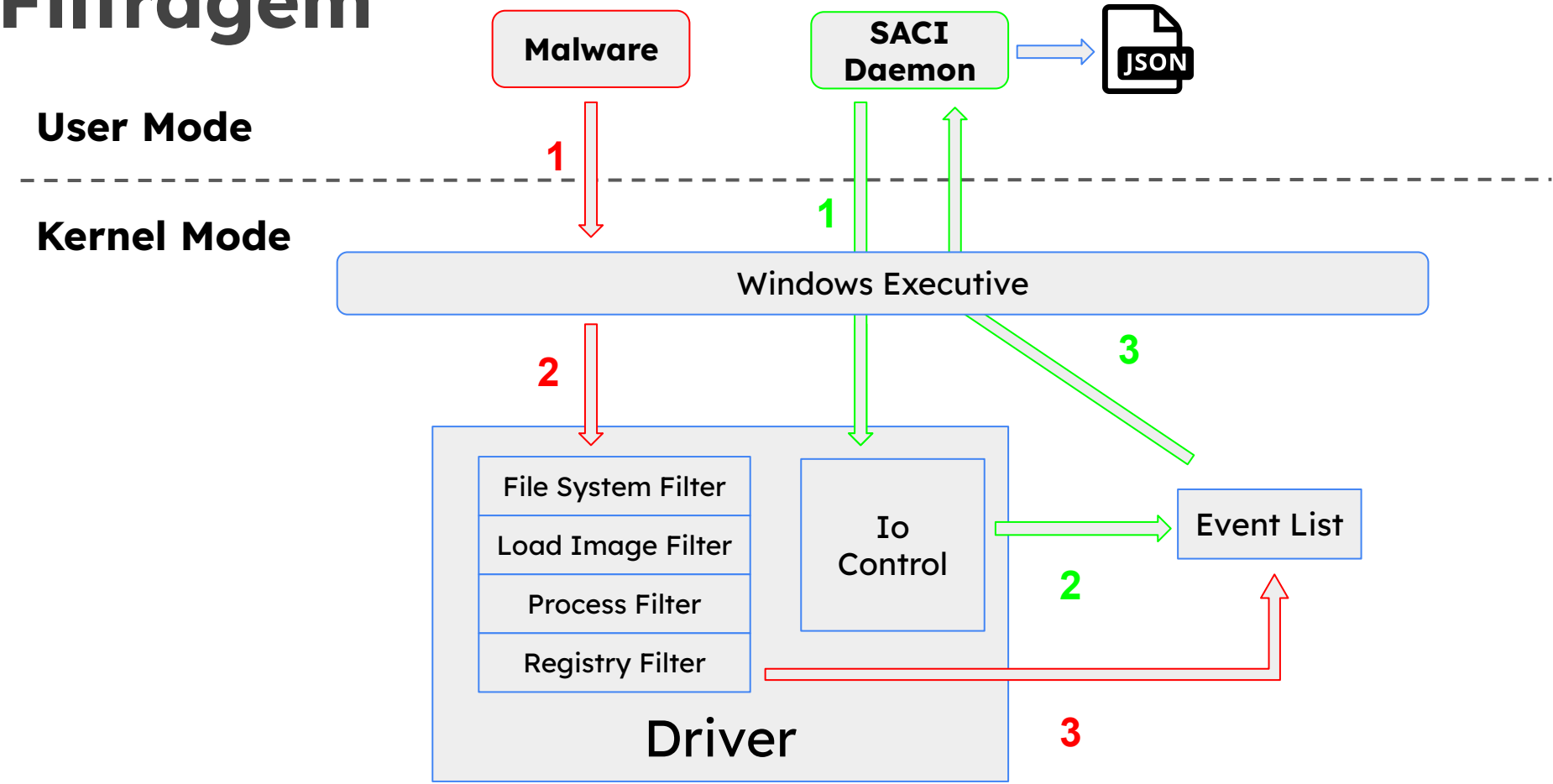
Filtragem


Malware
SACI Daemon
JSON
User Mode
Kernel Mode
1
1
Windows Executive
2
File System Filter
Load Image Filter
Process Filter
Registry Filter
Io Control
Event List
Driver
3

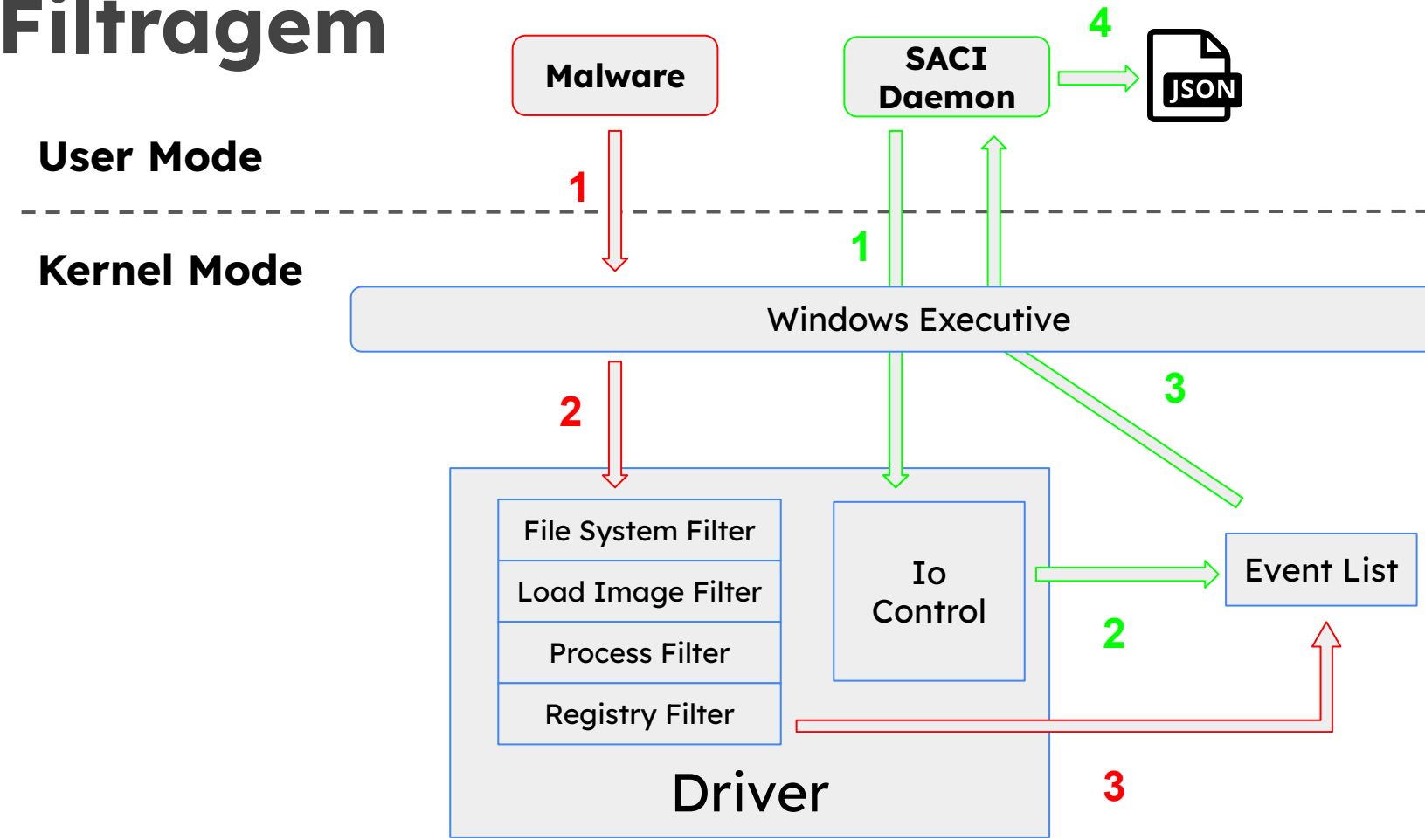
Filtragem


Malware
SACI Daemon
JSON
User Mode
Kernel Mode
1
1
Windows Executive
2
File System Filter
Load Image Filter
Process Filter
Registry Filter
Io Control
Event List
2
3
Driver

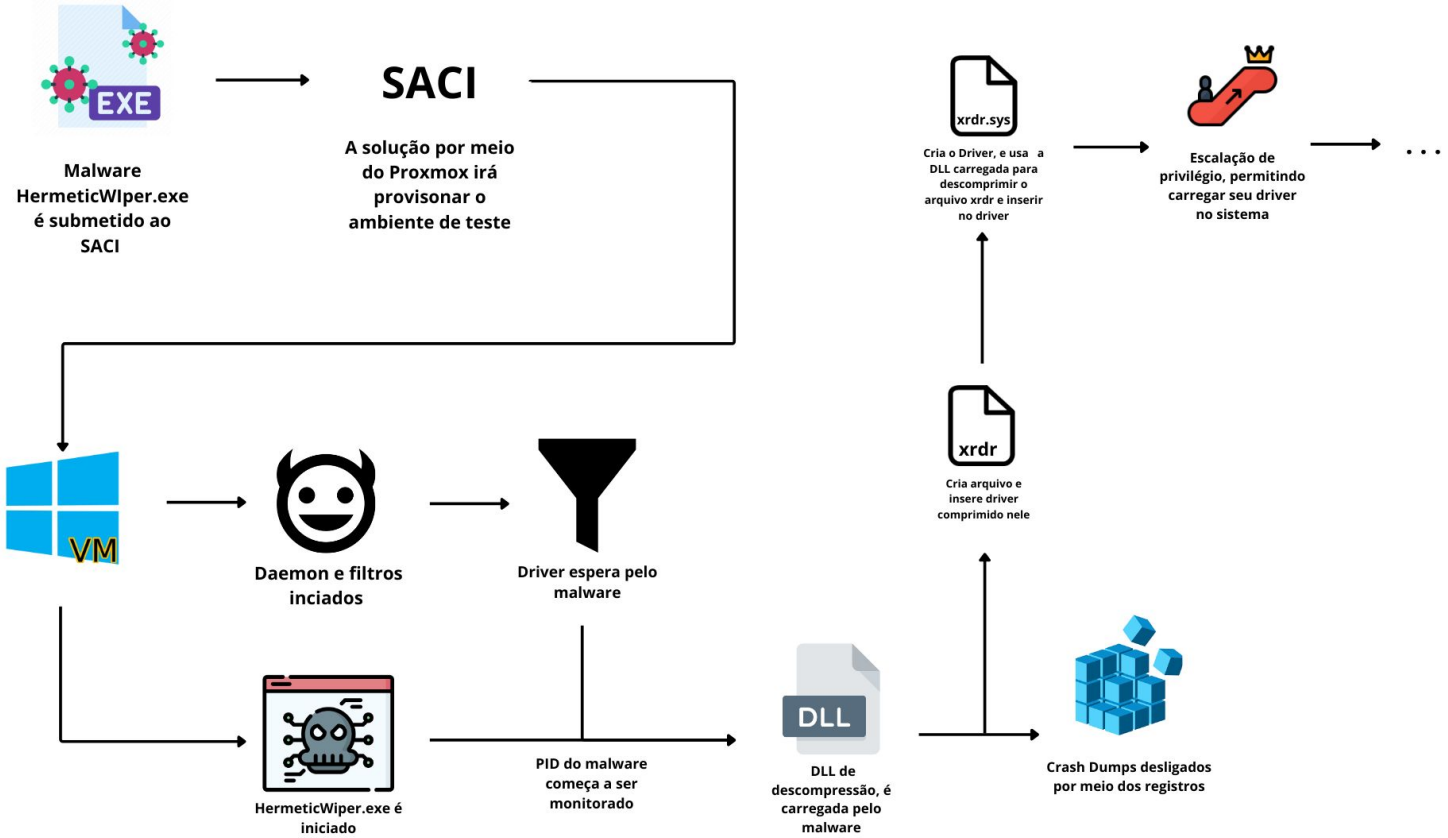
Filtragem


Malware
SACI Daemon
JSON
User Mode
Kernel Mode
1
1
Windows Executive
2
3
File System Filter
Load Image Filter
Process Filter
Registry Filter
Io Control
Event List
2
3
Driver

Filtragem


Malware
SACI Daemon
4
JSON
User Mode
1
Kernel Mode
1
Windows Executive
2
3
File System Filter
Load Image Filter
Process Filter
Registry Filter
Io Control
Event List
2
3
Driver

Estudo de Caso



Considerações finais

- Plataforma promissora para análise de malware multicomponente
  - Limitações
- Sandbox do SACI em estágio preliminar para análise automatizada em escala
  - Ambiente em construção

Trabalhos futuros

- Plataforma de virtualização anti-evasão
- Adição de novos filtros (ex.: handles, rede, etc.)
- Análise de memória
- Heurísticas para detecção do ações maliciosas
- Disponibilizar interface Web para testes públicos

Obrigado!

- Bernardo P. Tomasi, Davi C. Ribeiro, Pedro Friedrich, Ruibin Mei, Yago Furuta, Jorge Correia, André Grégio

- saci@c3sl.ufpr.br

Patrocinadores do SBSeg 2024!

nic.br

cgi.br

Google

Tempest

CAPES

SiDi

FAPESP

zscaler™

BugHunt

CNPq

C.E.S.A.R

FACULDADE IBPTECH