



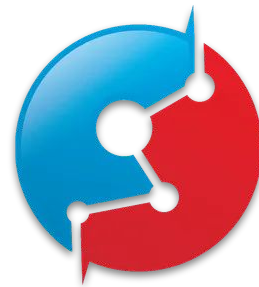
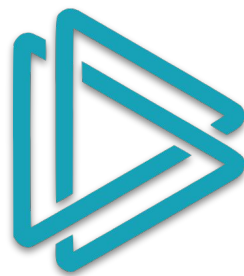
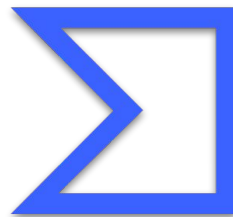
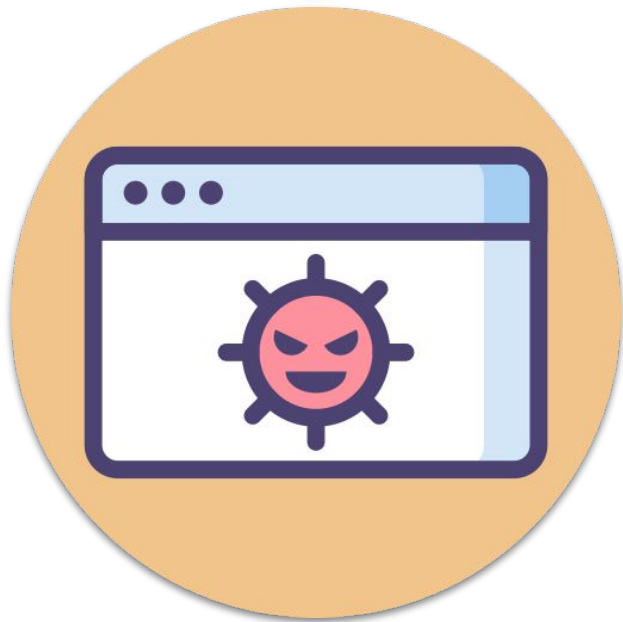
SACI: Solução Automatizada para Análise Comportamental de Código Infeccioso em SO MS Windows Modernos

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



Universidade Federal do Paraná

Motivação



Problema(s)

62/75 Community Score

62/75 security vendors flagged this file as malicious

0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da
TROJAN.WIN32.HERMETICWIPER

Size: 114.26 KB | Last Analysis Date: 13 days ago

DETECTION | DETAILS | RELATIONS | BEHAVIOR | COMMUNITY (30+)

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Display grouped sandbox reports

CZAE	0	0	0	0	0	0	0	0	0	0	0	CAPA	0	7	0	0	0	0	0	0	0
CAPE Sandbox	0	6	0	0	0	0	0	0	0	0	0	DAS-Security Orcas	1	5	0	0	0	0	0	0	0
Lastline	2	0	0	0	0	0	0	0	0	0	0	Microsoft Systeminternals	0	0	0	0	0	0	0	0	99+
Rising MOVES	0	0	0	0	0	0	0	0	0	0	0	Tencent HAO	0	0	0	0	0	0	0	0	0
VirusTotal Jujubox	0	0	0	0	0	0	0	0	0	0	0	VirusTotal Observer	0	0	0	0	0	0	0	0	0
Yomi Hunter	1	8	0	0	0	0	0	0	0	0	0	Zenbox	2	7	0	0	0	0	0	0	17

Activity Summary | Download Artifacts | Full Reports | Help

2 Detections | 1 Mitre Signatures | 1 IDS Rules | 0 Sigma Rules | 4 Dropped Files | 1 Network Comms

Process and service actions ⓘ

Permissions Requested

- SE_LOAD_DRIVER_PRIVILEGE

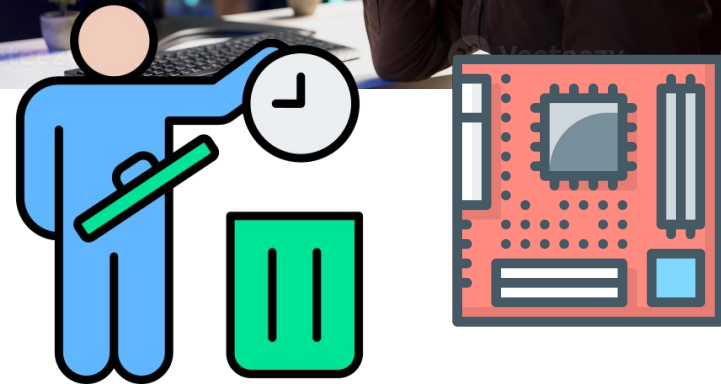
Processes Created

- {SamplePath}\0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da.exe
- C:\Users\Elijah\AppData\Local\Temp\0031140146.exe
- C:\Users\Elijah\AppData\Local\Temp\0385eeab00e946a302b24a91dea418230450f5ece21da.exe
- C:\Users\Mason\AppData\Local\Temp\0385eeab00e946a302b24a91dea418230450f5ece21da.exe
- C:\WINDOWS\system32\Drivers\rhdr.sys
- C:\Windows\system32\Drivers\dbdr.sys
- C:\Windows\system32\Drivers\hzdr.sys
- %SAMPLEPATH%\0385eeab00e946a302b24a91dea4187c1210597b8e17cd9e2230450f5ece21da.exe
- %SAMPLEPATH%\84ba0197920fd3e2b7dfa719fee09d2f.exe
- C:\Windows\System32\wuapihost.exe



Superficialidade

Problema(s)



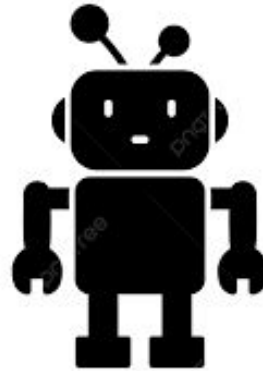
Setup trabalhoso e demorado

Desafio(s)

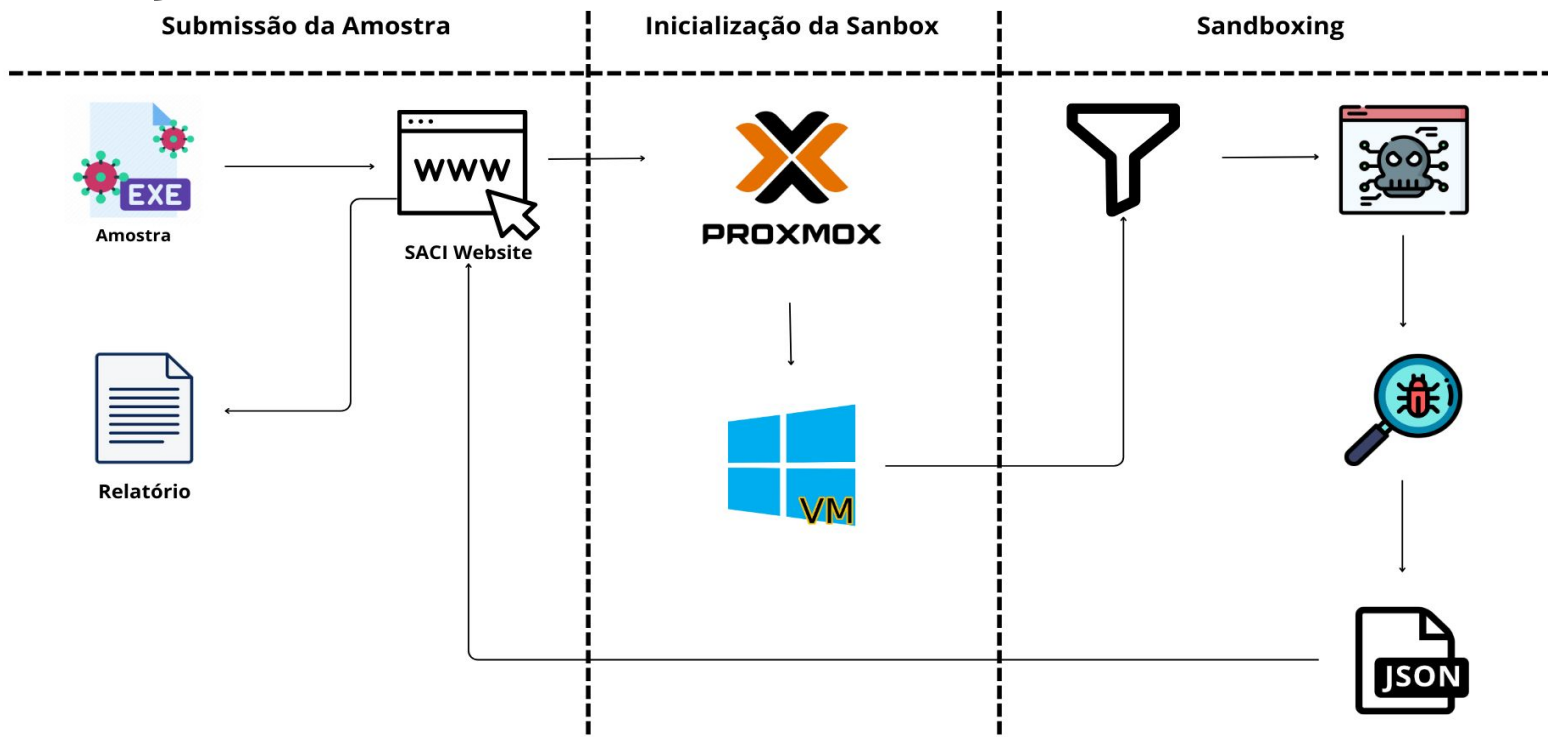
Encontrar um meio termo entre a profundidade da análise e automação



VS

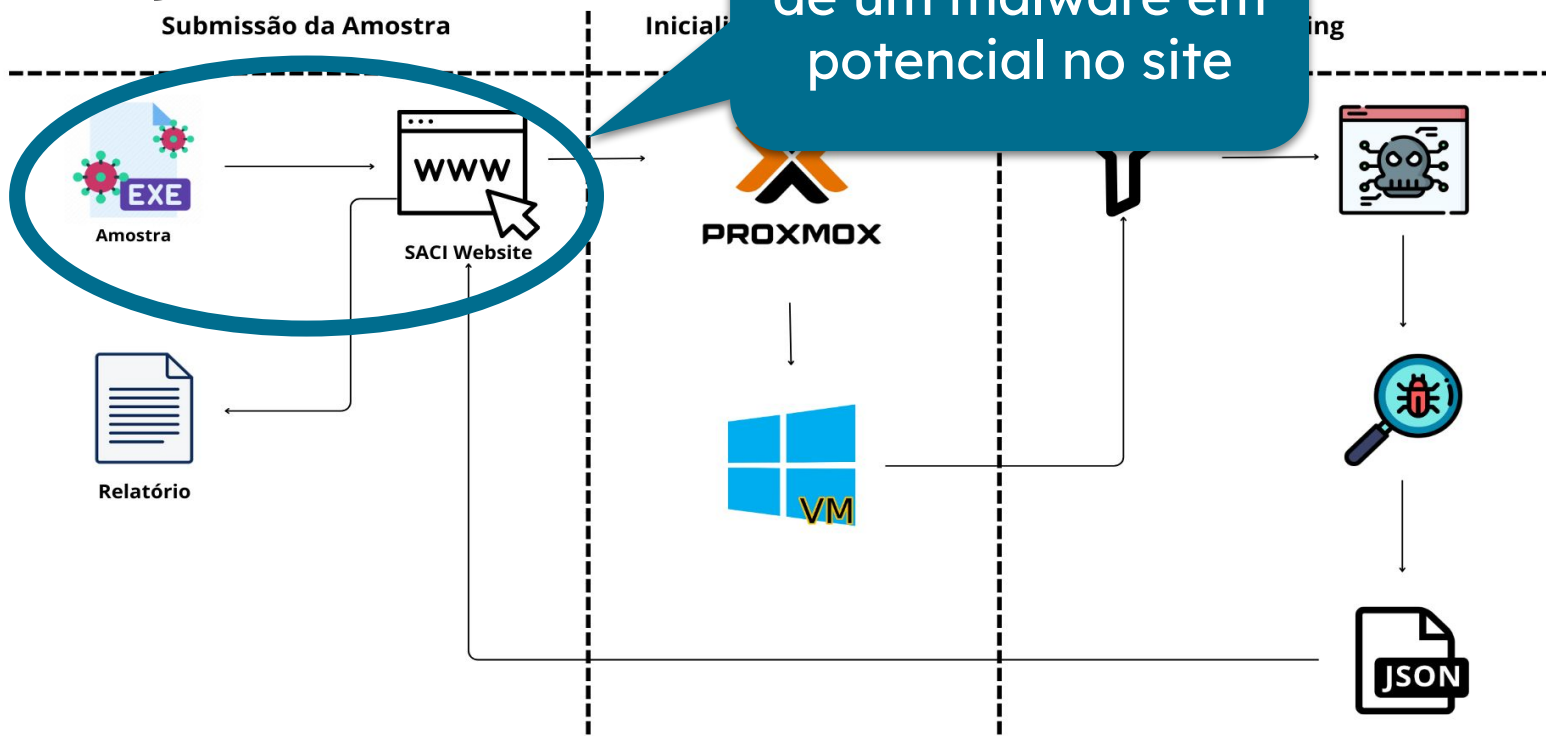


Solução Proposta

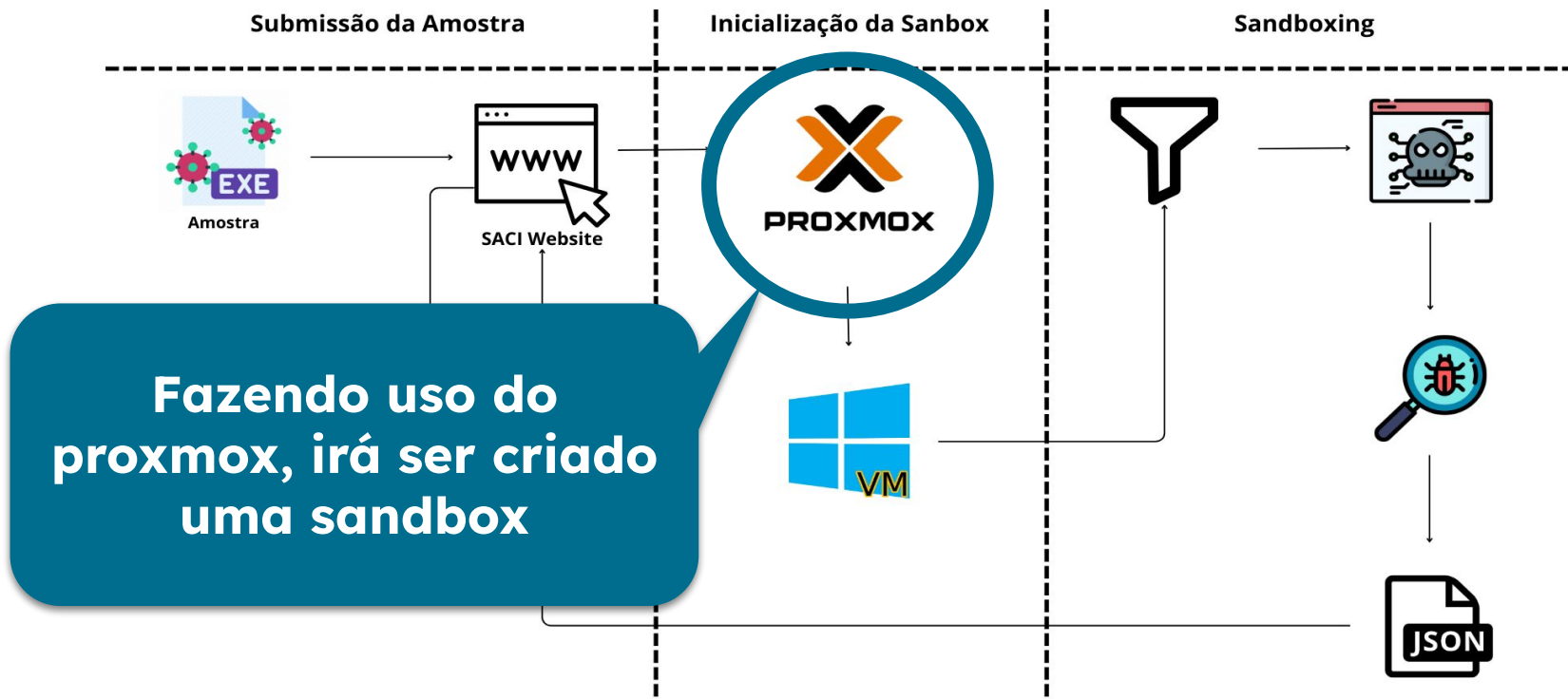


Solução Proposta

Submete a amostra de um malware em potencial no site



Solução Proposta

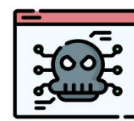


Solução Proposta

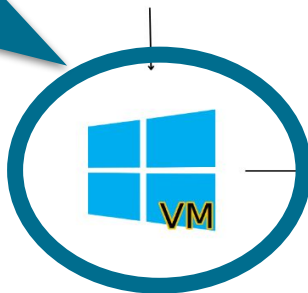
Submissão da Amostra

Inicialização da Sandbox

Sandboxing



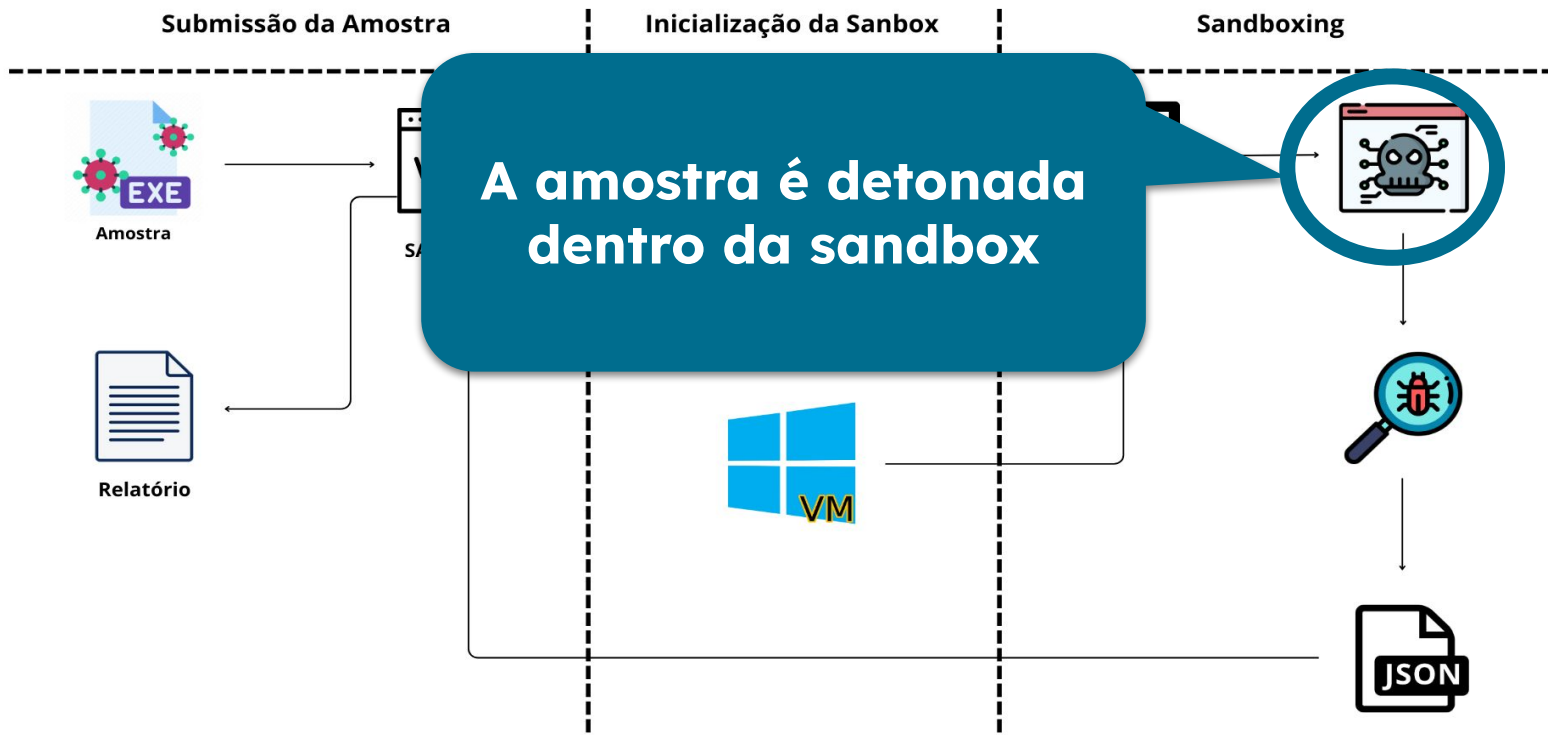
Uma Sandbox de Windows 10/11 é criada com o aparato de filtragem



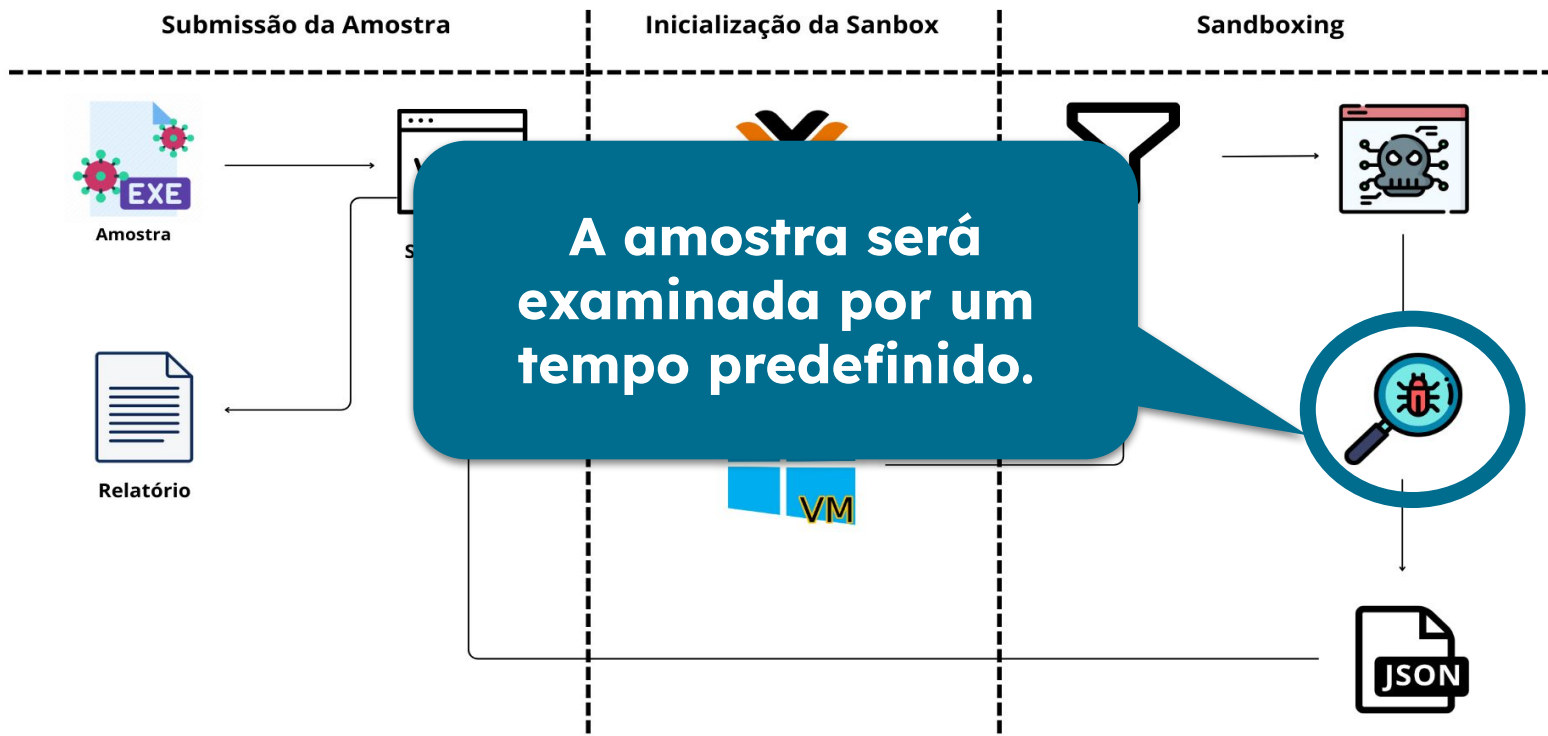
Solução Proposta



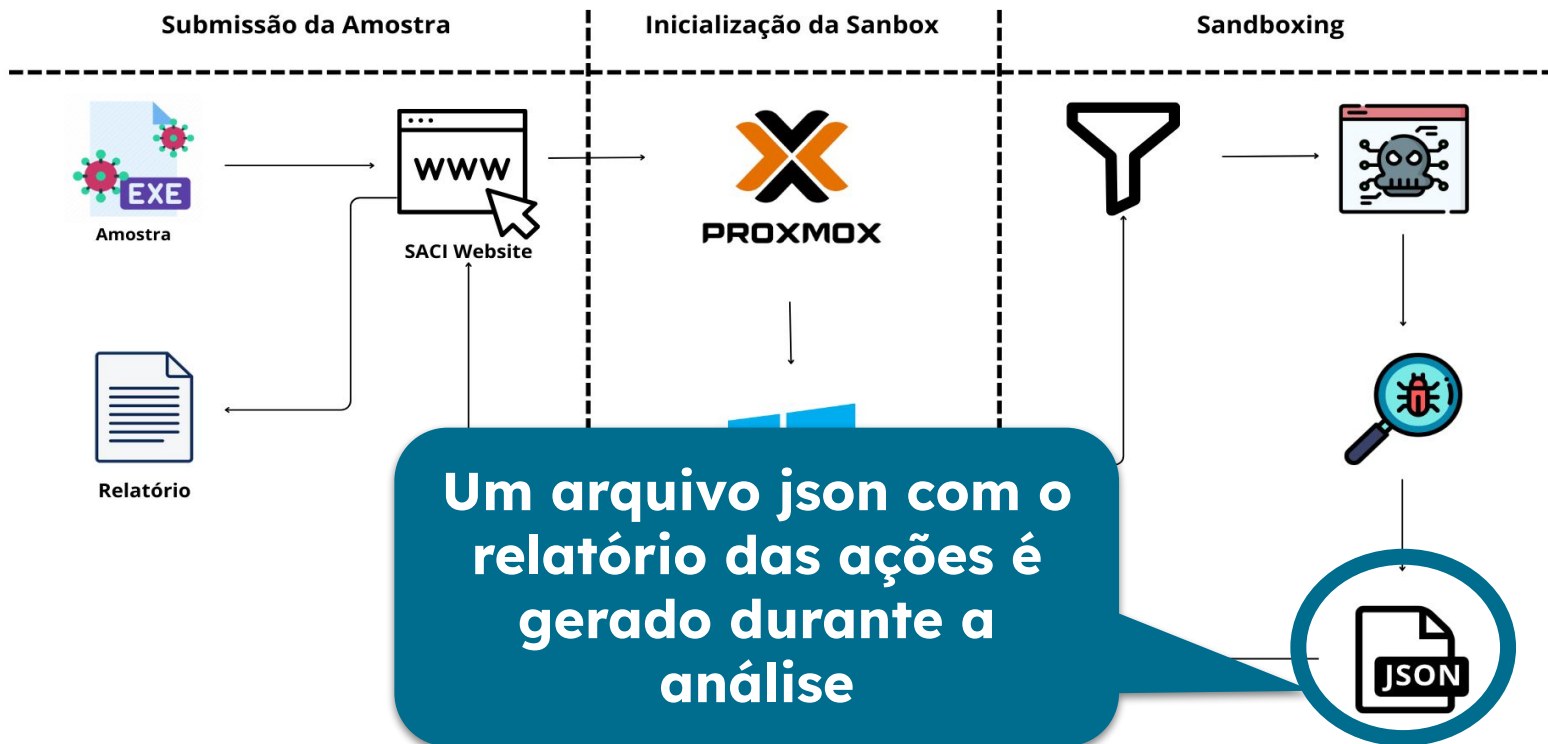
Solução Proposta



Solução Proposta



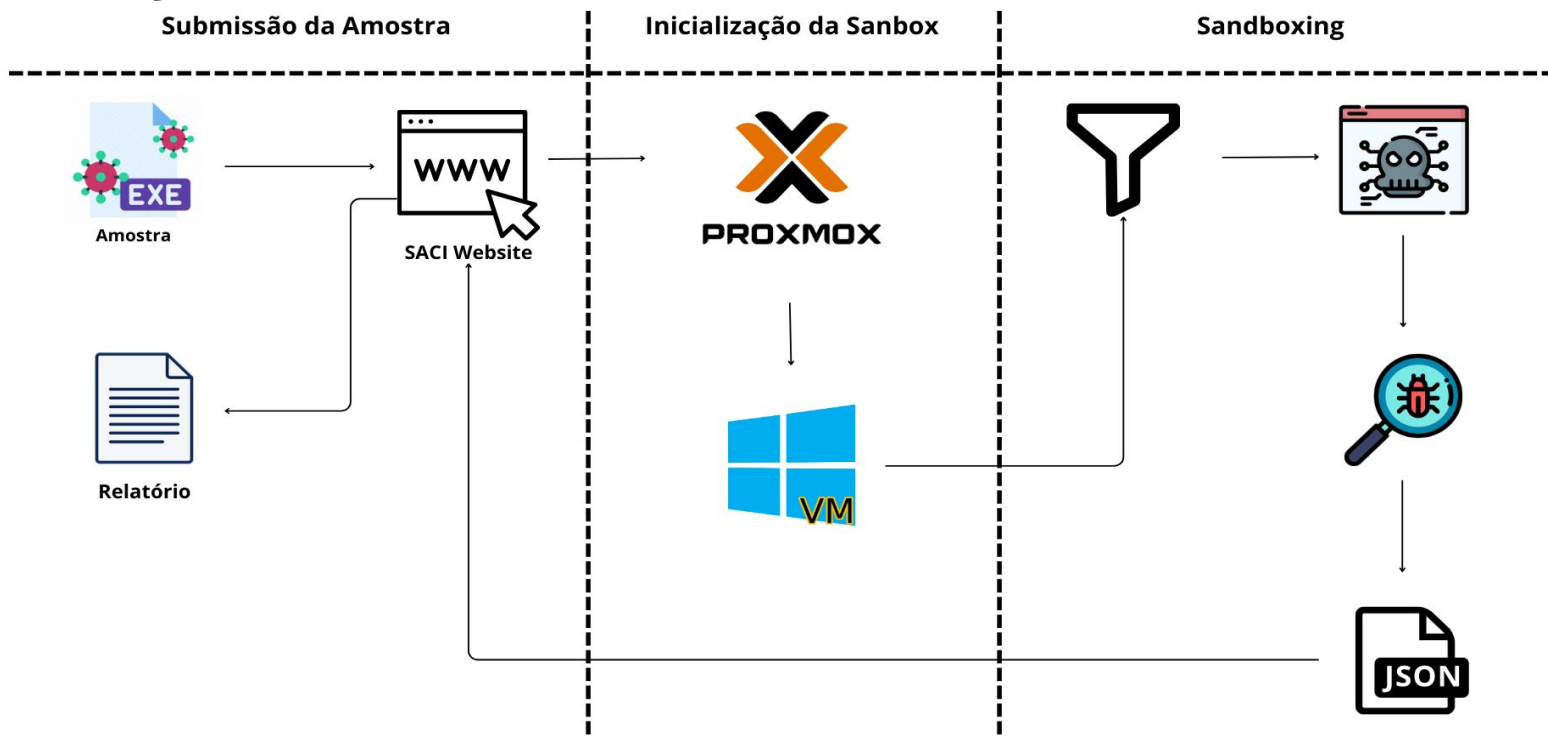
Solução Proposta



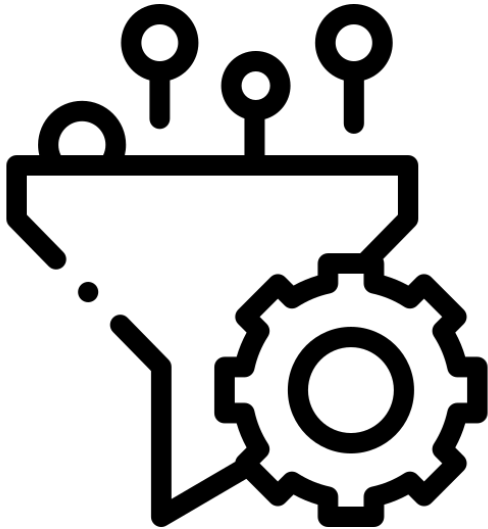
Solução Proposta



Solução Proposta



Filtragem



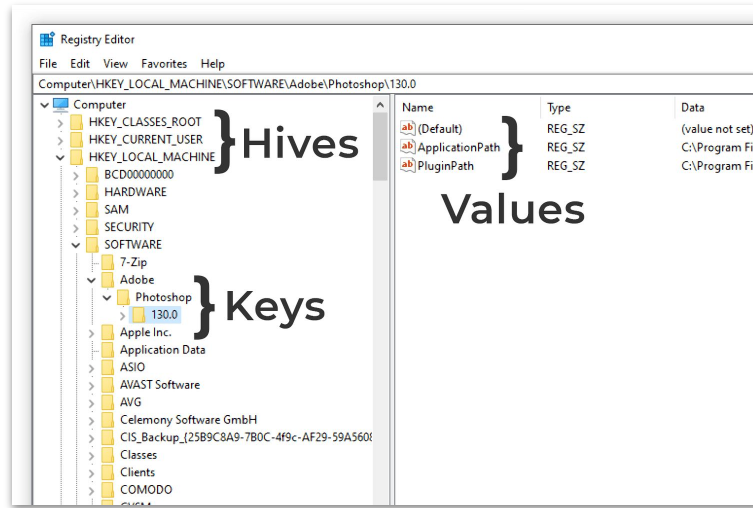
Driver de Filtragem:

- 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

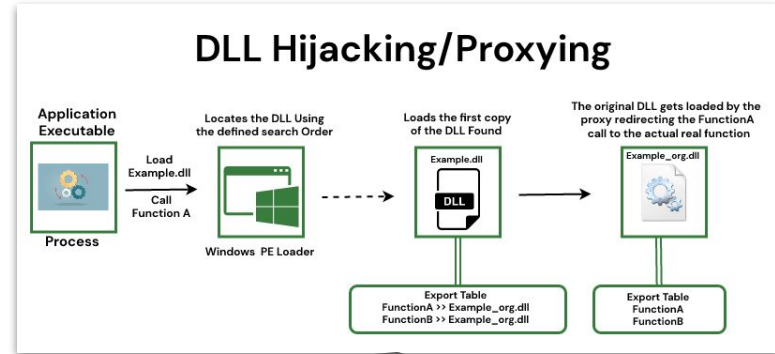


```
{  
  "date": "4/9/2024",  
  "time": "11:31:19:143",  
  "info type": "INFO_REG",  
  "registry operation": "RegNtSetValueKey",  
  
  "name": "\\REGISTRY\MACHINE\SOFTWARE\WOW6432Node\Microsoft\Tracing\malware_RASAPI32",  
  "data type": "REG_DWORD",  
  "data": "0 0 0 0"  
}
```

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

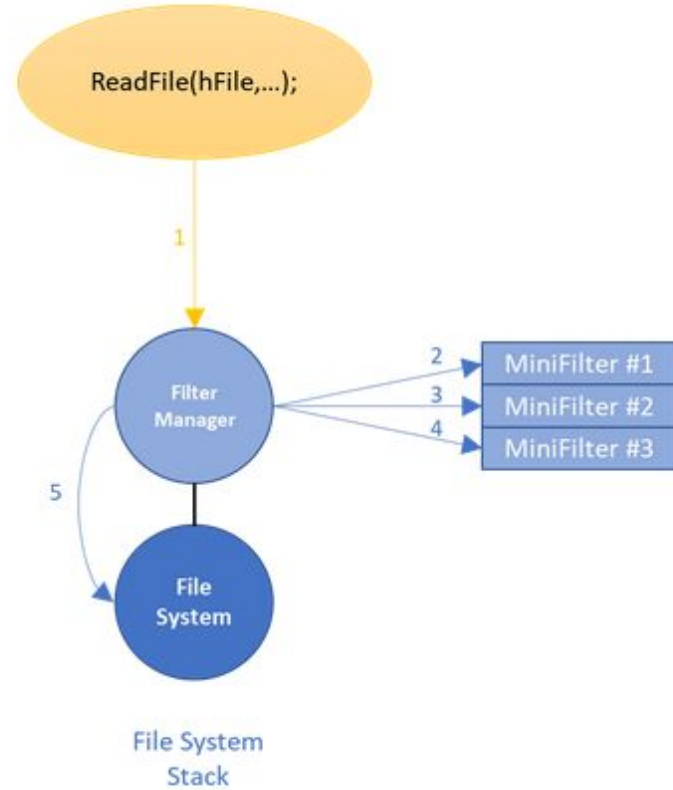
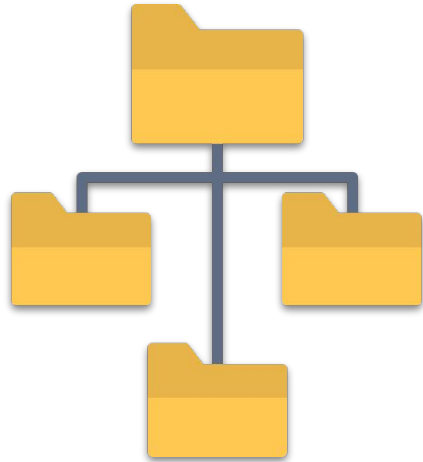
Side-loading

Spoofing

Carregamento de imagens

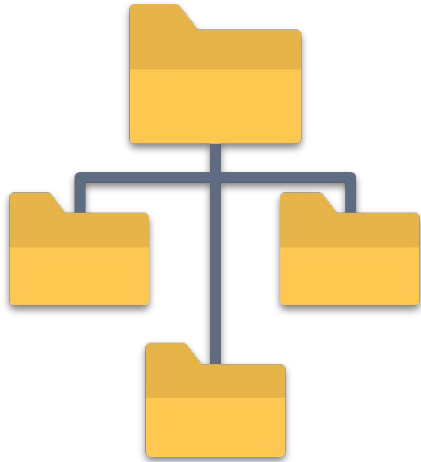


Filtragem



Evento de sistema de arquivos

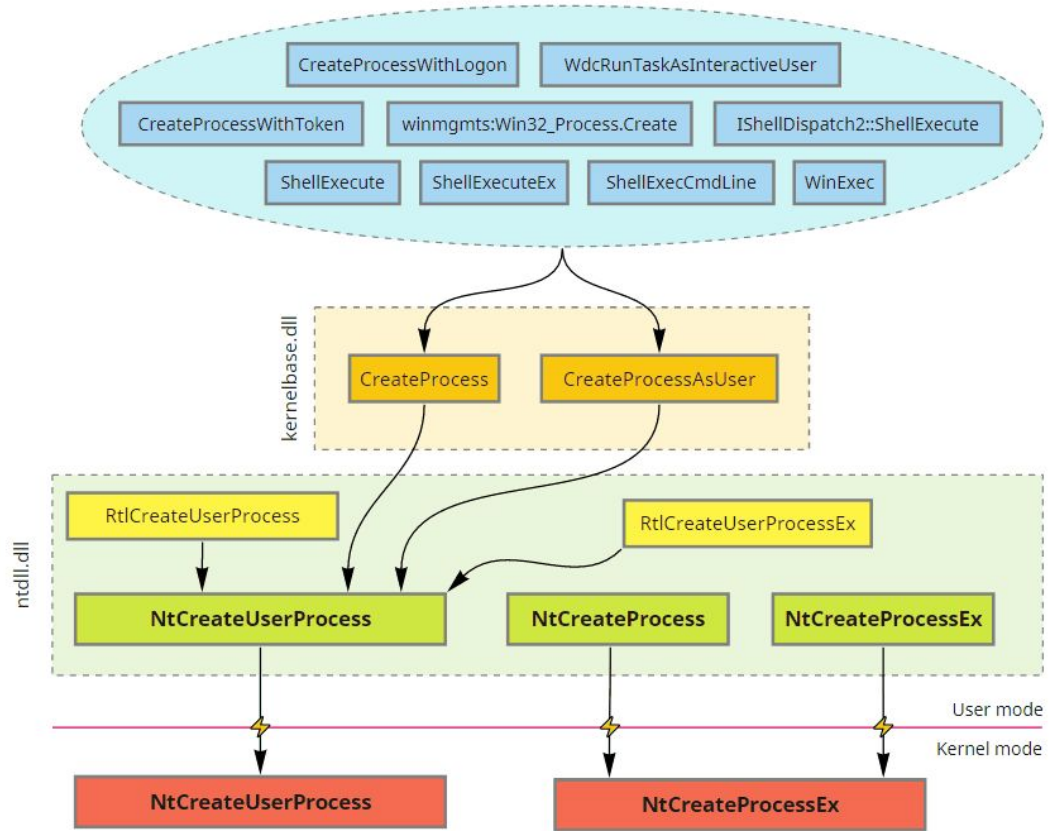
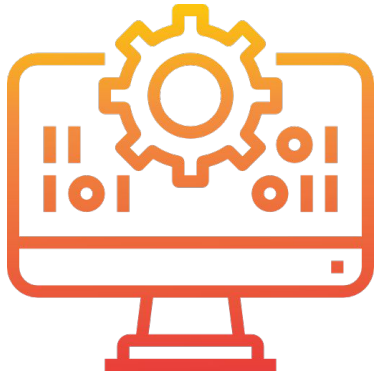
Filteragem



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

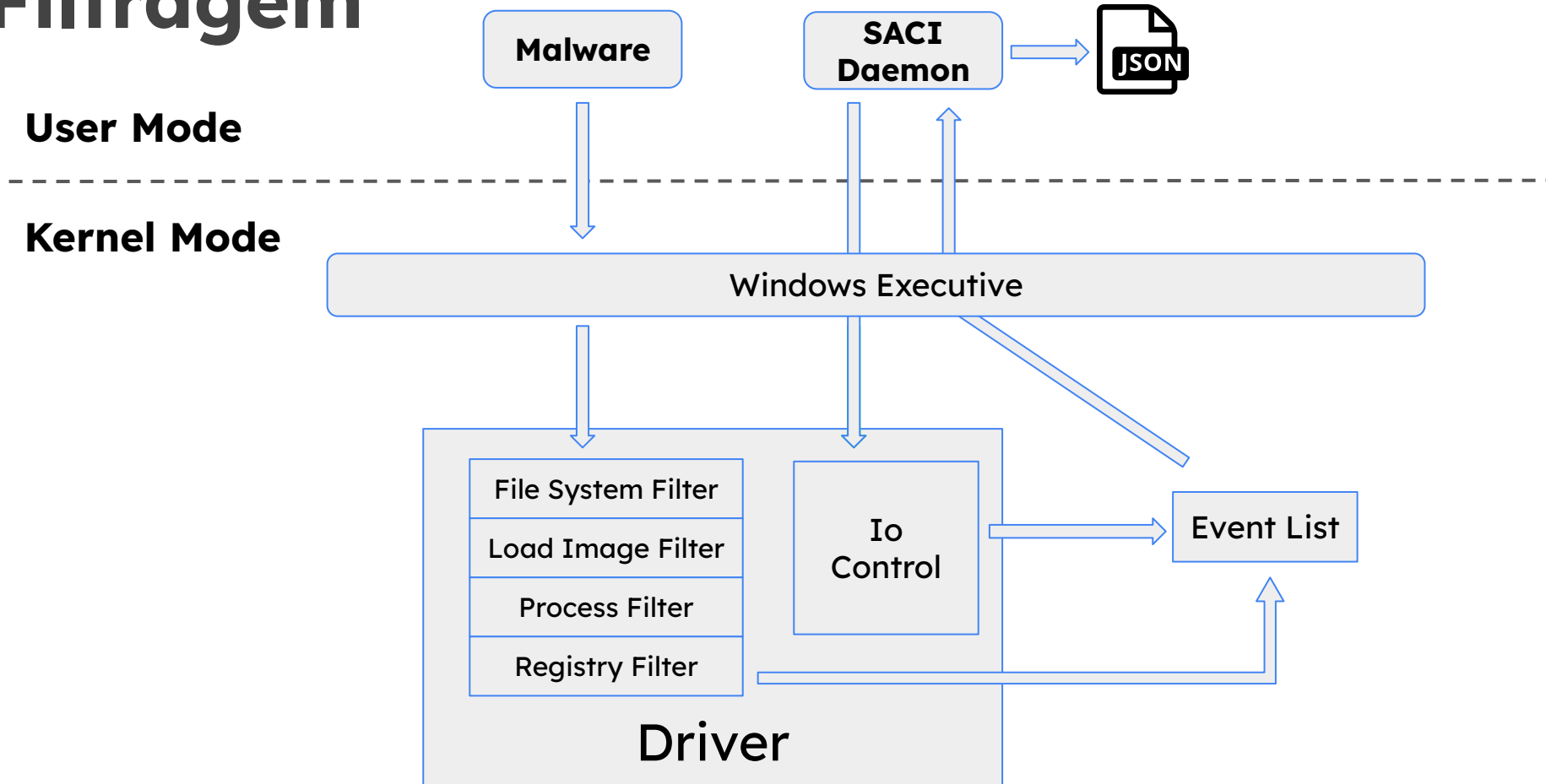
Filteragem



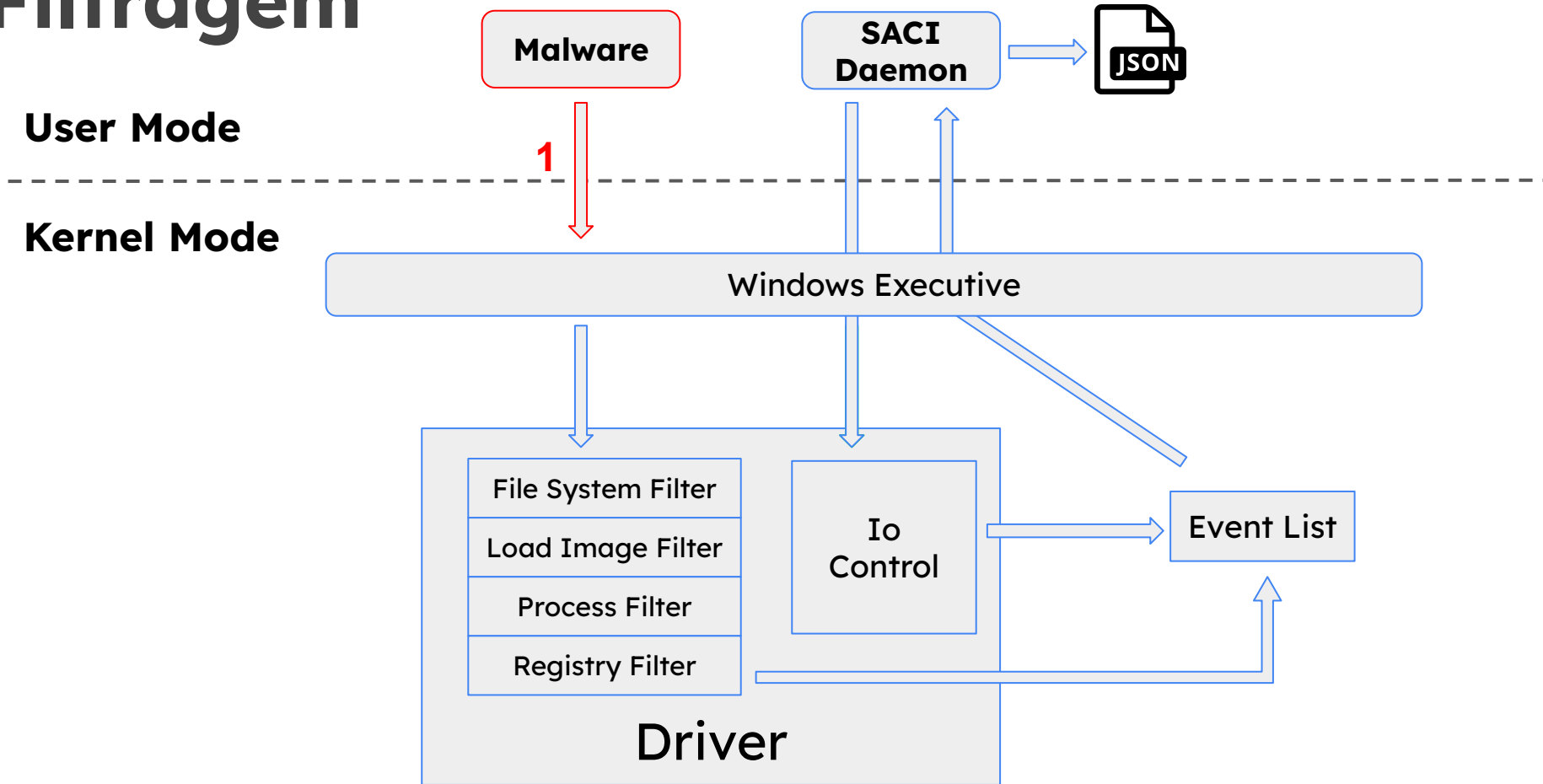
Log

```
{
  "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"}
  ]
}
```

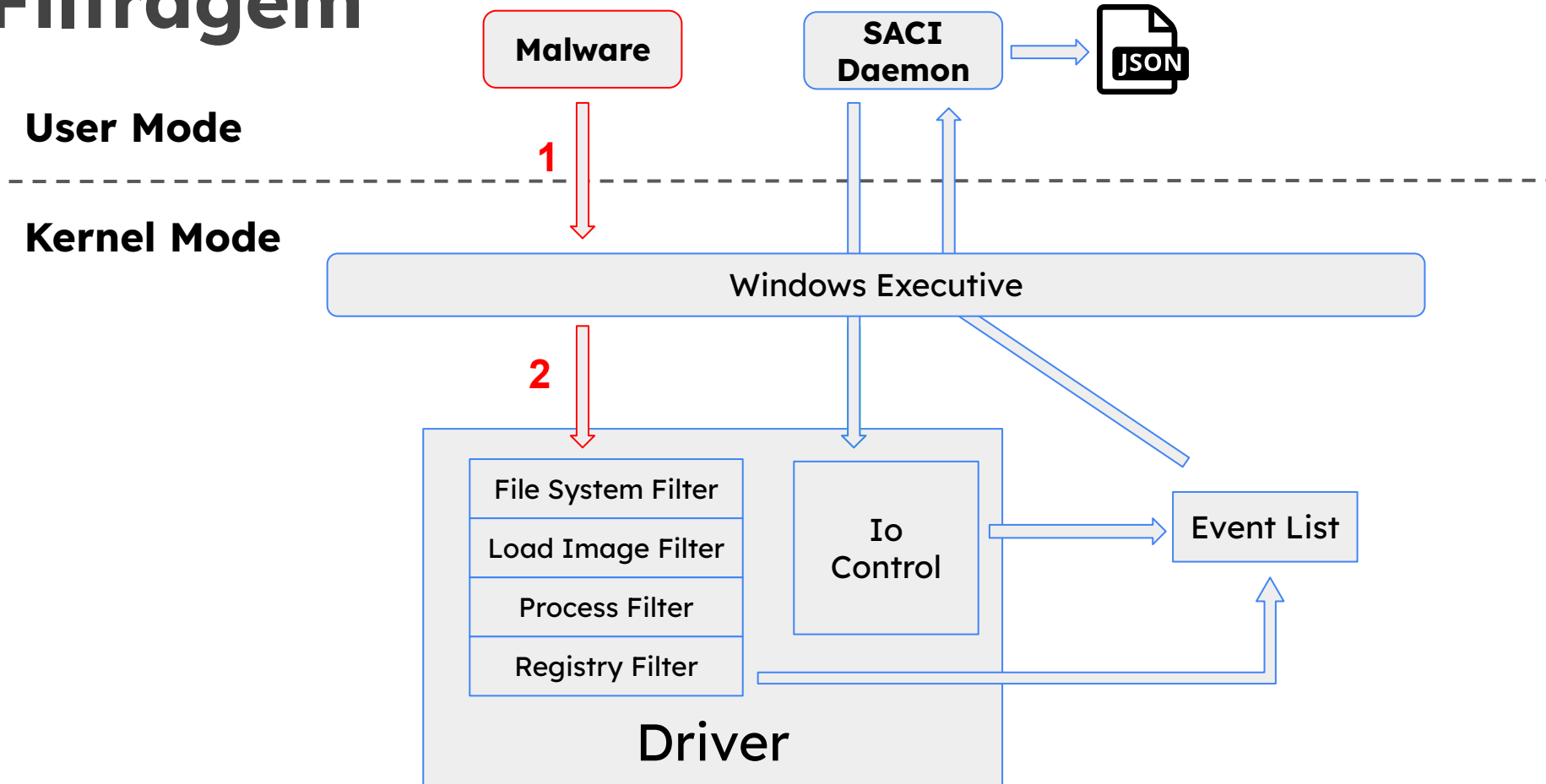
Filtragem



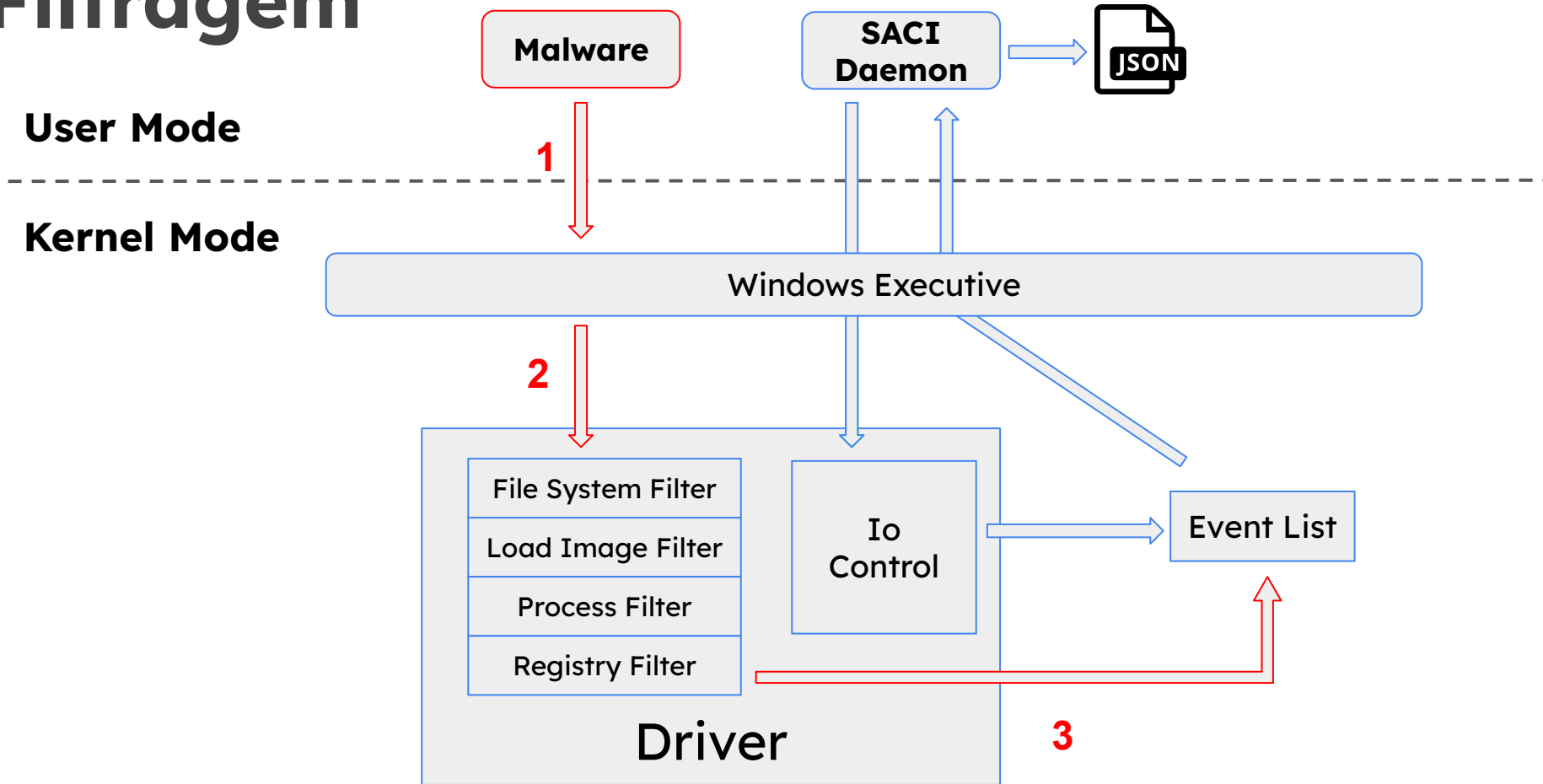
Filtragem



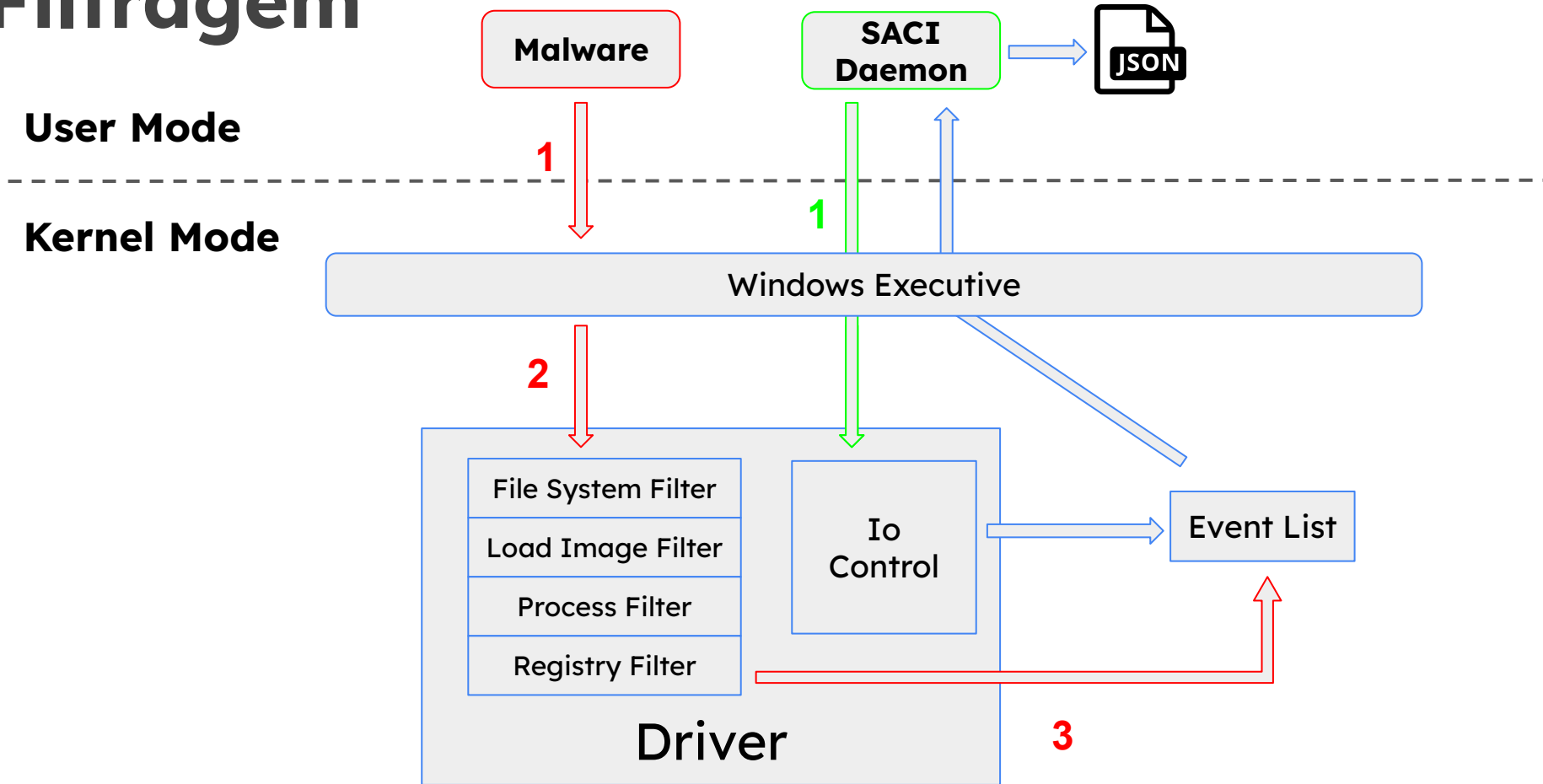
Filtragem



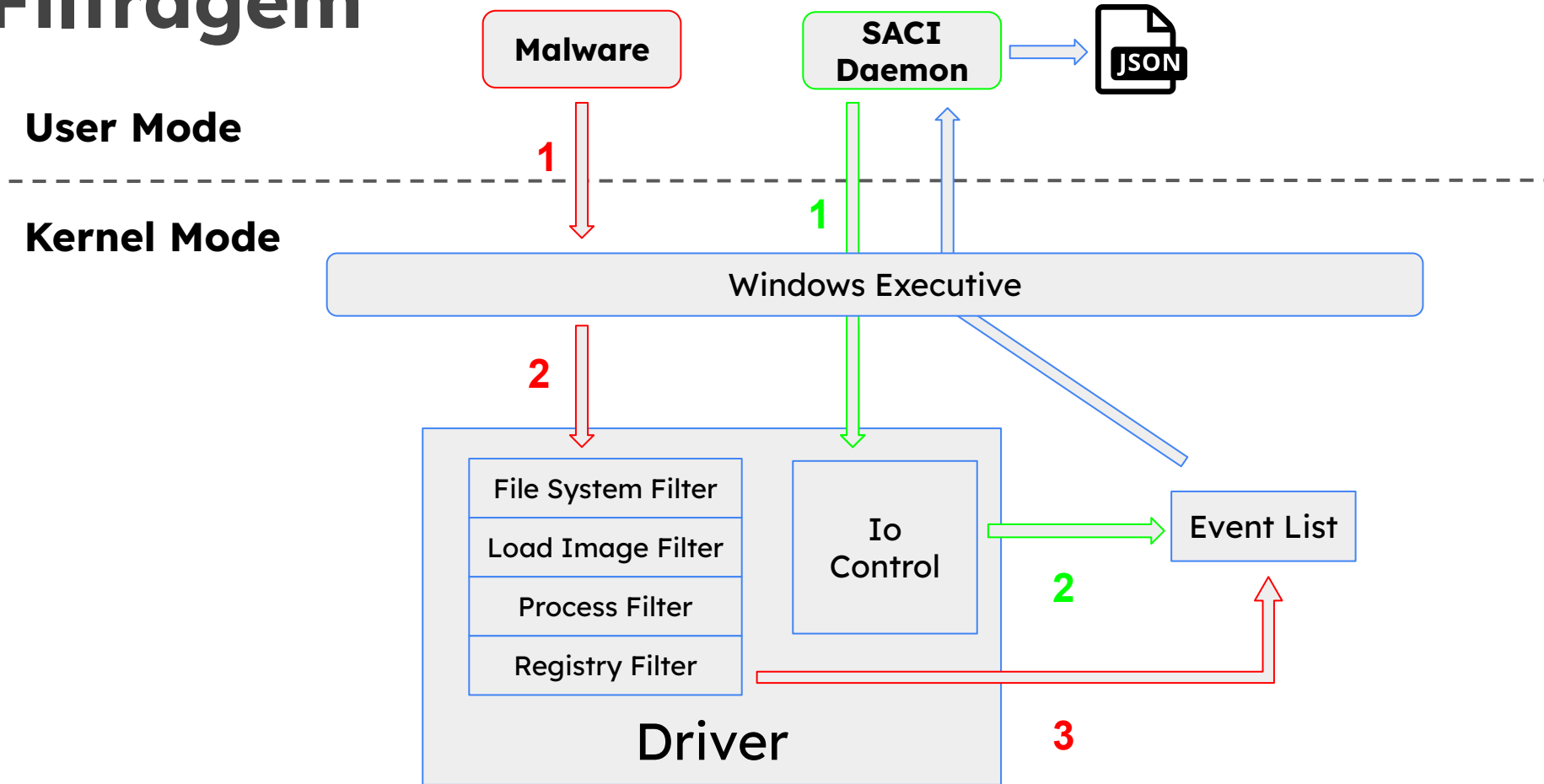
Filtragem



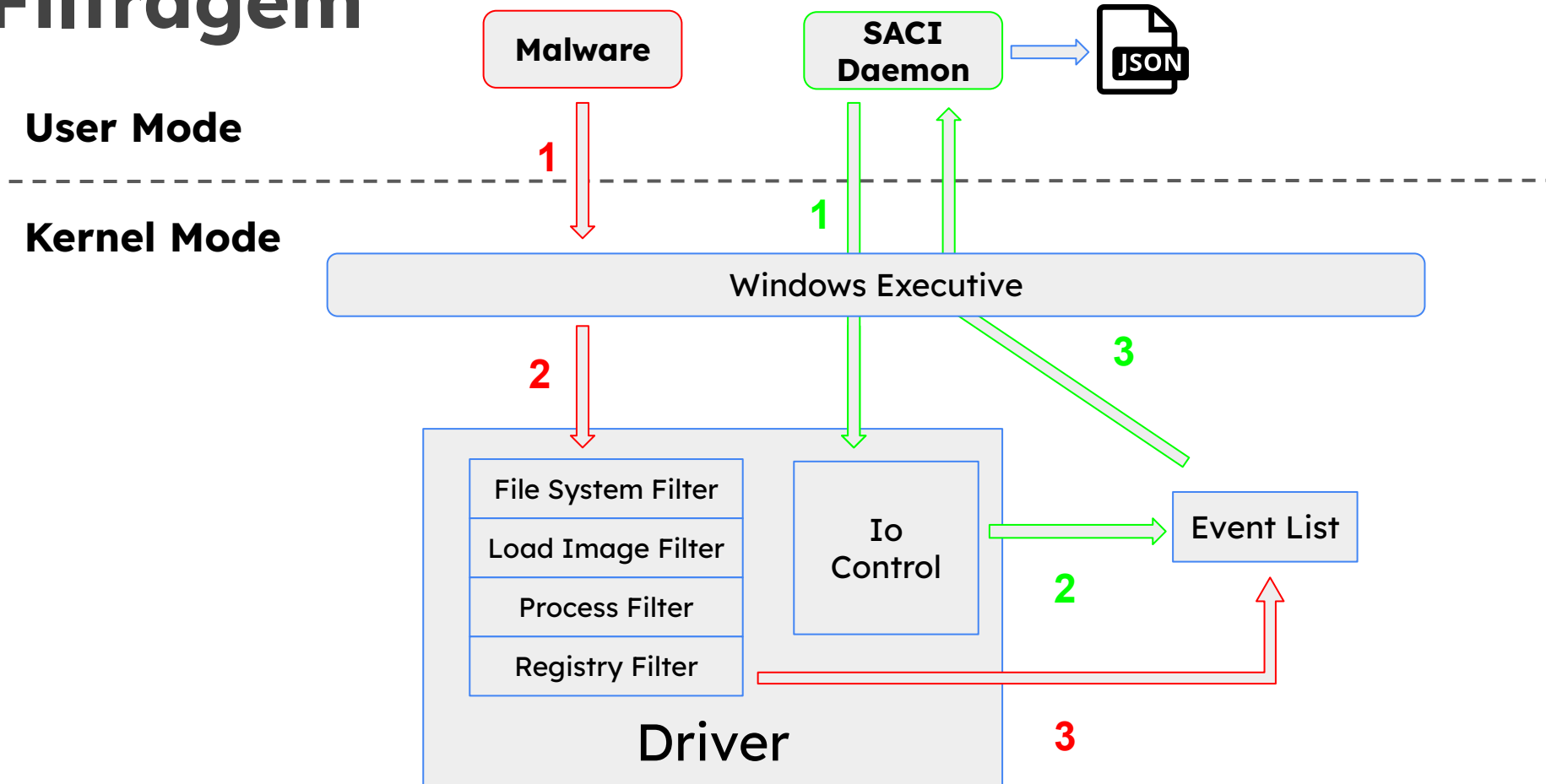
Filtragem



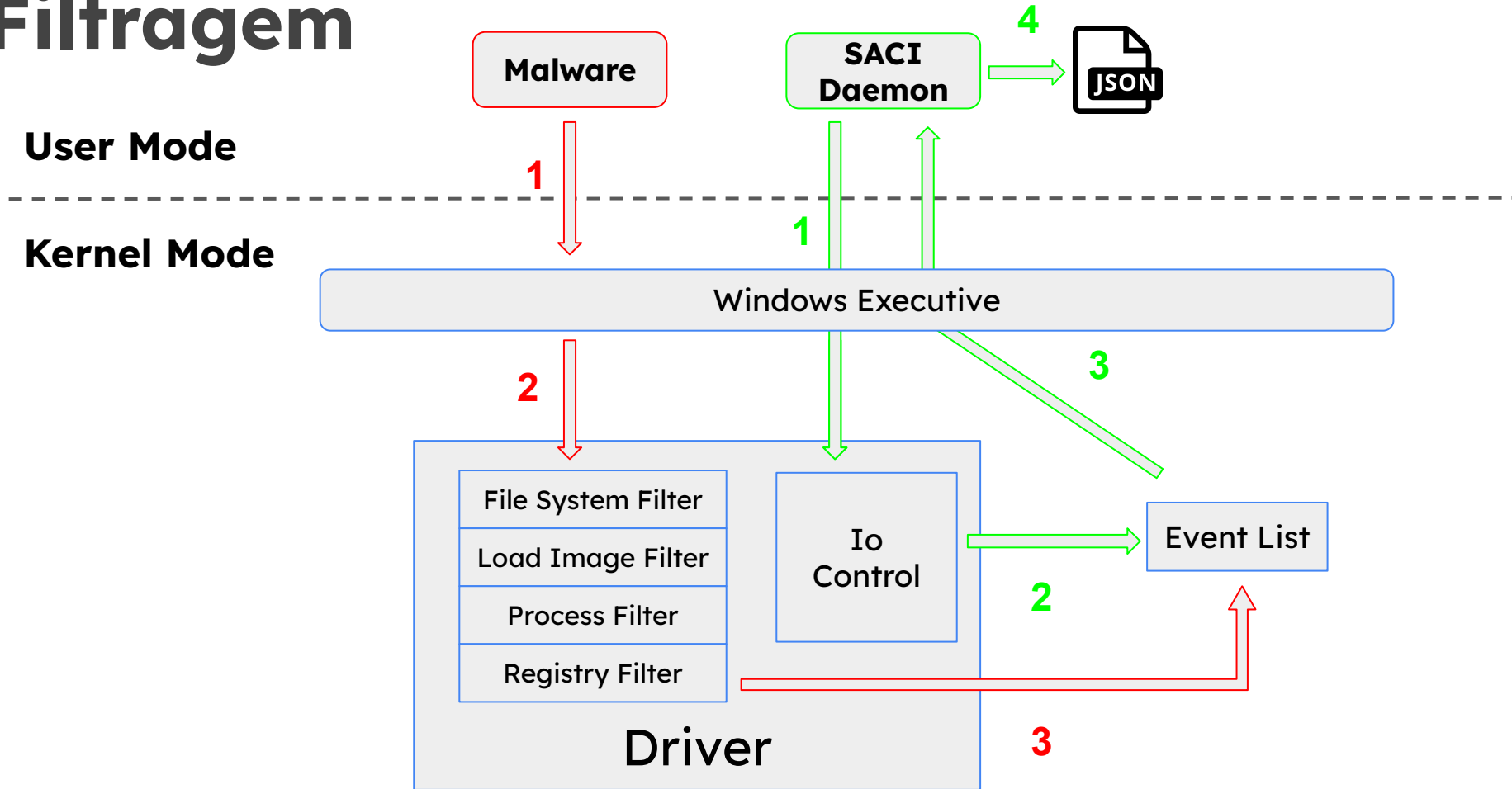
Filtragem



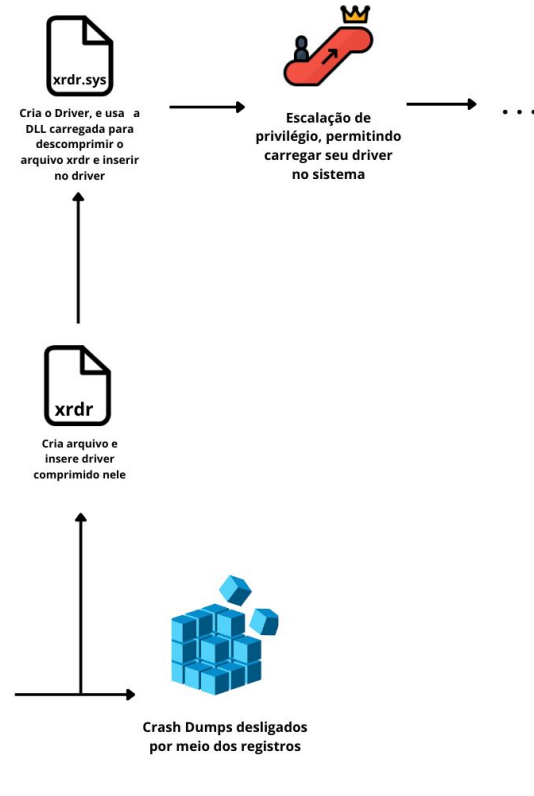
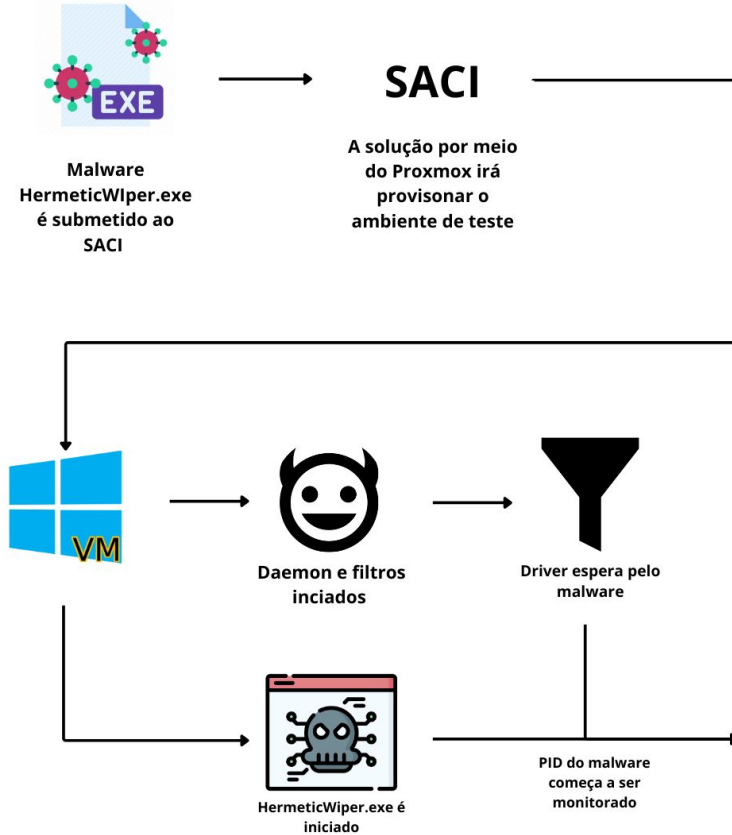
Filtragem



Filtragem



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 de 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

SECRET

./C3SL
UFPR





Patrocinadores do SBSeg 2024!

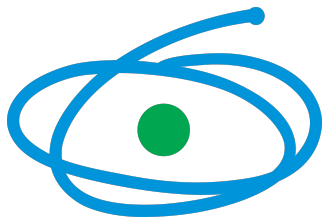
nie.br

egi.br

Google



Tempest



CAPES



SiDi



FAPESP



CNPq



C.E.S.A.R



zscaler™



BugHunt



FACULDADE
IBPTech