PARDED - Uma ferramenta de detecção passiva de malwares com foco em rootkits que utilizam técnicas de ofuscação de tráfego

Maickel J. Trinks[1]
Mateus Terra[2]
João Gondim[2]

[1]CEPESC
[2]UNB

17 de setembro de 2024

SBSeg24 SÃO JOSÉ DOS CAMPOS

CEPESC

Sumário

Introdução

Motivações

- Detecção de códigos maliciosos com desenvolvimento direcionado, visando obtenção de informações
- Foco no Governo - Informações com classificação de sigilo
- Técnicas inexistentes em sistemas tradicionais

Características

Capacidade de ocultar presença
Utilizados por grupos APT
Acesso privilegiado no sistema operacional
Controle remoto pelo atacante
Instalação de softwares

Questionamentos:

- Sistemas Tradicionais de defesa: efetividade
- Detecção de ofuscação de informações: destino
- Automatização da detecção
- Diferenciar tráfego legítimo de malicioso/ofuscado
- Gerar inteligência: CTI

Objetivos:

- Estruturar uma arquitetura de detecção por *rootkits*
- Ser complementar a sistemas de defesa existentes;
- Gerar inteligência através do correlacionamento e enriquecimento dos dados de detecções;
- Gerar resultados de fácil interpretação.

Sumário

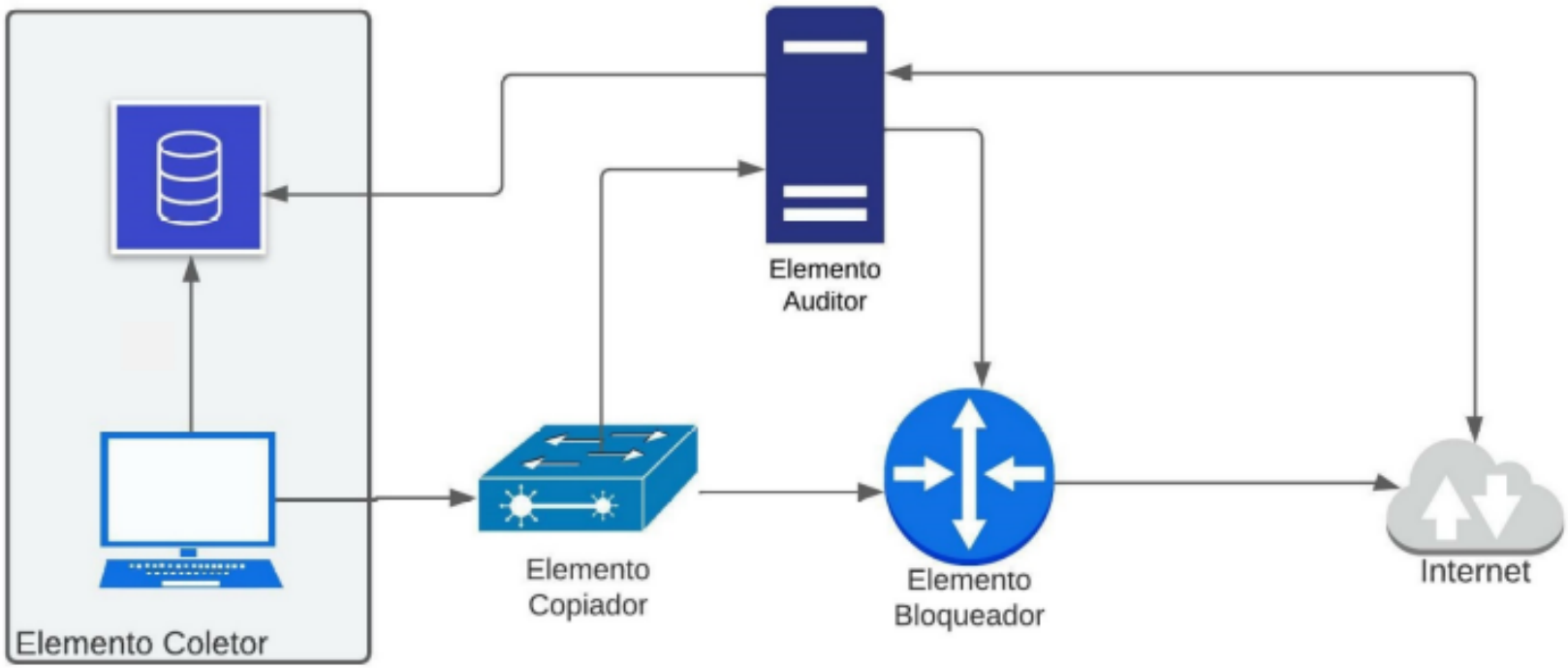


Figura: Arquitetura PARDED

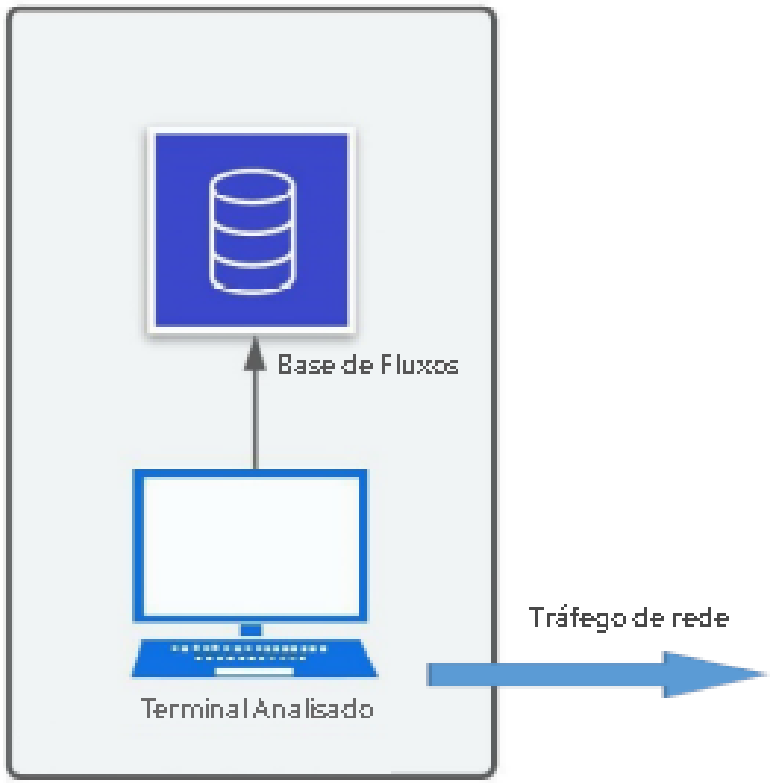


Figura: Elemento Coletor

Fluxo Transmitido$^{(1)}$
$\neq$
Base de Fluxos

$^{(1)}$ Com ofuscação ativa

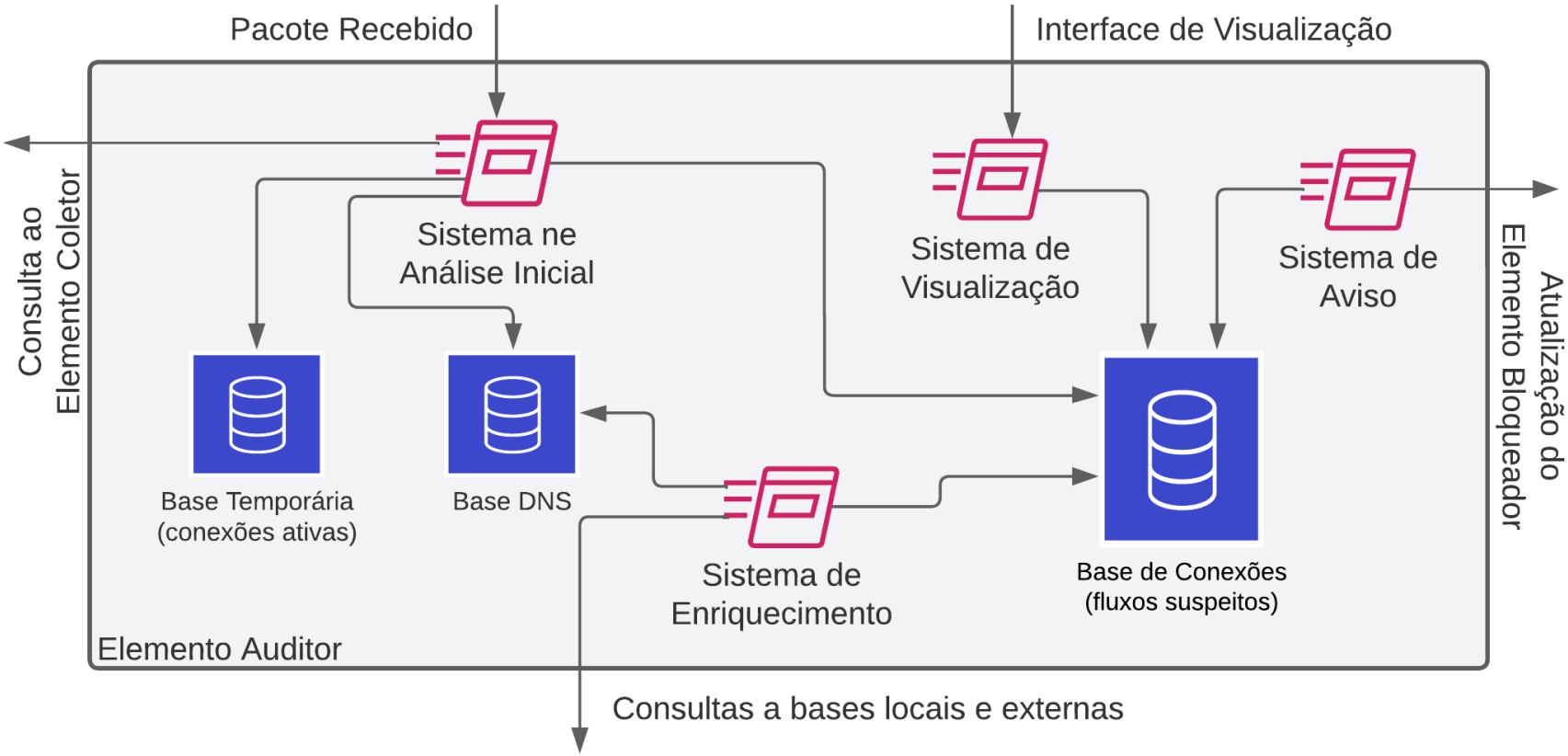
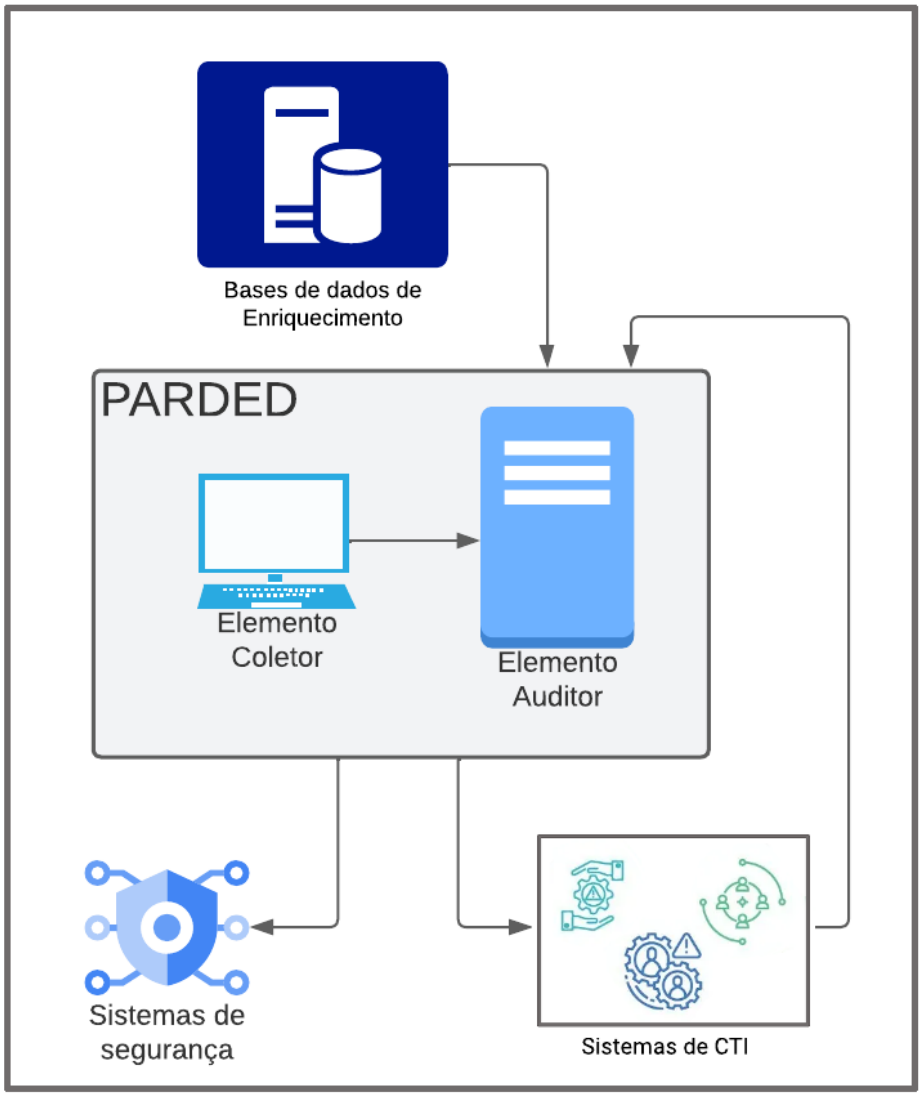


Figura: Elemento Auditor

PARDED

Arquitetura



Sumário

Testes

Fluxos legítimos e maliciosos

Tempo de resposta do sistema (sem atuação do rootkit).

Tipo de Processamento	Característica do Fluxo	Média de Pacotes	Tempo de processamento (ms)	Tempo de processamento com carga de 50Mbps(ms)
Sem consulta ao Coletor	Na base Temporária	55.393	0,00110	0,00100
	Resposta DNS	2030	0,00407	0,00734
Com consulta ao Coletor	Fluxos Legítimos	983	516,78	551,05

Tempo de resposta do sistema pra fluxos exclusivamente suspeitos.

Tipo de Processamento	Característica do Fluxo	Média de Pacotes	Taxa (pacotes por segundo)	Tempo de processamento (ms)
Com consulta ao Coletor	Fluxos Suspeitos	100	1 pps	1.742,77
		100	10 pps	1.674,18
		500	10 pps	1.838,37

Testes

Fluxos legítimos e maliciosos

Tempo de resposta do sistema (com atuação do rootkit).

Tipo de Processamento	Característica do Fluxo	Pacotes Transmitidos	Tempo de processamento (ms)	Tempo de processamento com carga de 50Mbps(ms)
Sem consulta ao Coletor	Na base Temporária	54.058	0,00114	0,00100
	Resposta DNS	1.329	0,0370	0,00730
Com consulta ao Coletor	Fluxos Legítimos	684	536,15	561,26
	Fluxos Suspeitos	100	1.642,64	1.709,62

Ações do Sistema de Enriquecimento.

Tipo de processamento	Descrição da Base de Dados	Número de Consultas	Resposta (ms)
Consulta à base local	Nó pertencente a rede TOR	100	42,18
Consulta à base remota	Plataforma VirusTotal	30	1.241,14

Ações do Sistema de Aviso.

Tipo de processamento	Número de Consultas	Resposta (ms)
Sem bloqueio (limiares não atingidos)	50	9,31
Com bloqueio (limiares atingidos)	50	89,60

Sumário

Conclusões

Arquitetura

A arquitetura PARDED apresenta como resultados:

- estrutura escalável, generalizável e adaptável
- impactos pouco significantes no desempenho *
- enriquecimento de dados de múltiplas fontes
- dados de múltiplos terminais
- integração em sistemas existentes
- visualização de dados em interface única

Conclusões

Resultados

Resultados obtidos em laboratório:

- Tempo de resposta médio de 100 milissegundos [(1)]
- 95% dos pacotes processados em menos de 0,0012 ms [(1)]
- Não houve falsos negativos/positivos (marcação como suspeito)
- Atualizações em base remota inferior a 1,5 s [(2)]
- Atualizações em base local inferior a 50 ms
- Criação de regras inferior a 90 ms

(1) Configuração de tráfego utilizada: 0,17% malicioso, 2,3% dns, 70 pkt por fluxo

(2) API Virustotal

SBSeg24 SÃO JOSÉ DOS CAMPOS

CEPESC

Muito obrigado!

https://github.com/maickelj/parded
https://youtu.be/MBCC6ZzzPZk
https://youtu.be/oCjbl4vpyO8

maickeljosue@yahoo.com.br
maickel.1118@dte.gov.br

gondim@unb.br

SBSeg24 SÃO JOSÉ DOS CAMPOS

CEPESC