Análise estática de malware com o pev

OWASP FLORIPA DAY!

Fernando Mercês

$ whoami

Consultor Jequiti... ops, de segurança
BachareLANDO em CS
Sopa de letrinhas certified
Ativista FOSS

Agenda

O projeto pev
Obtendo informações de binários
Identificando binários maliciosos
Futuro do projeto

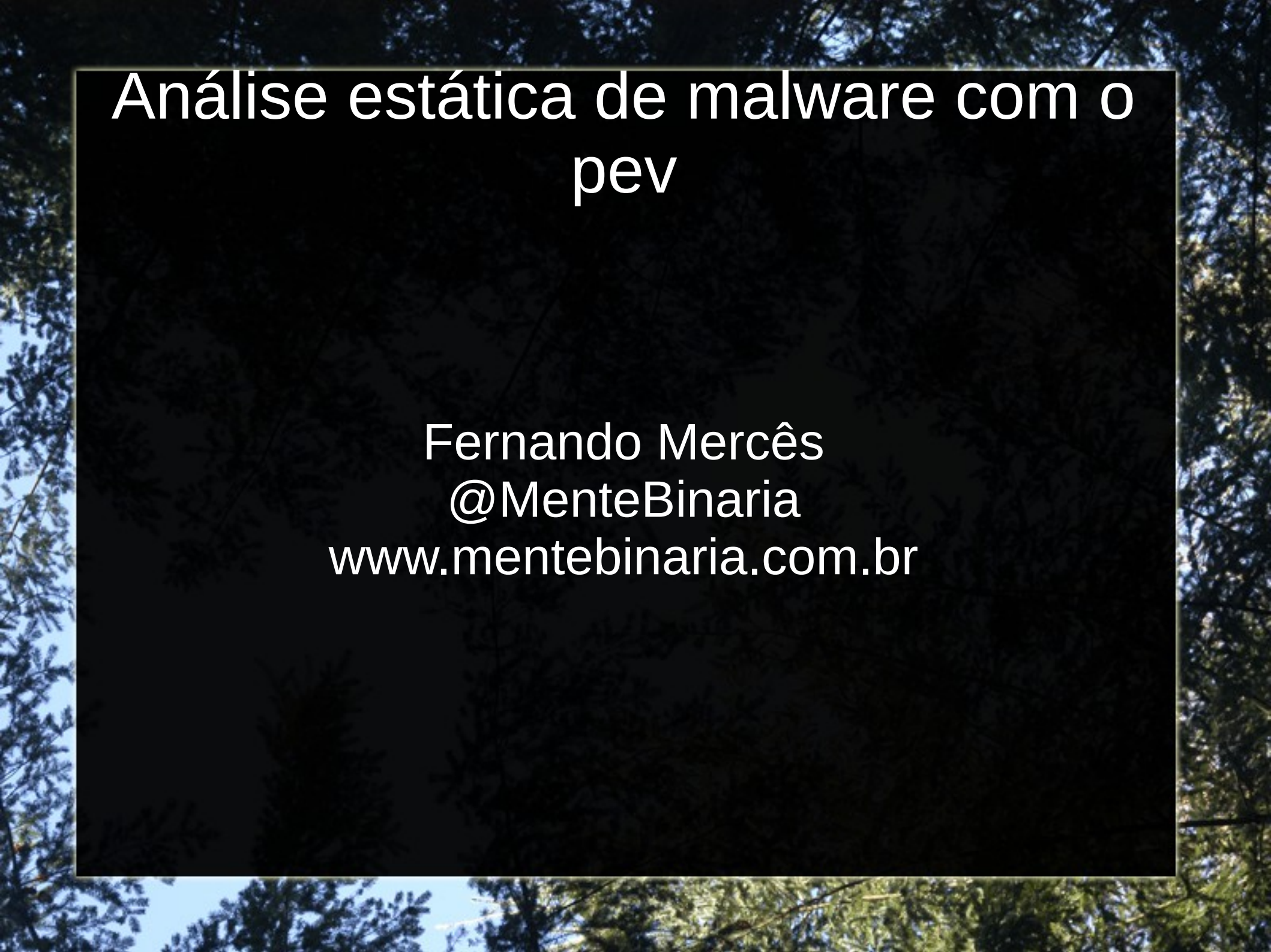
pev

Baseado na libpe
Foco em segurança
Multiplataforma
Não depende da API do Window$

Tals is cheap! VAMU VÊ!

pev

readpe
pedis
pepack
rva2ofs
pesec
pescan
pestr
pehash



Análise estática de malware com o pev

Fernando Mercês
@MenteBinaria
www.mentebinaria.com.br