UFAM

unipampa

Universidade Federal do Pampa

Ferramentas de extração de características para análise estática de aplicativos Android

Jonas Pontes, Estevão Costa, Vanderson Rocha, Nicolas Neves, Eduardo Feitosa, Joner Assolin e Diego Kreutz

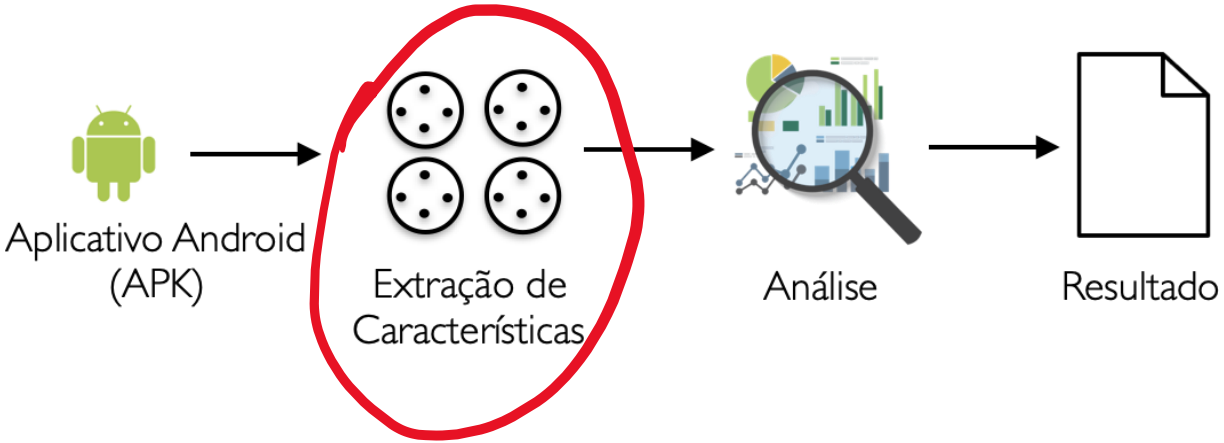
6º. Workshop Regional de Segurança da Informação (2021)

Contexto

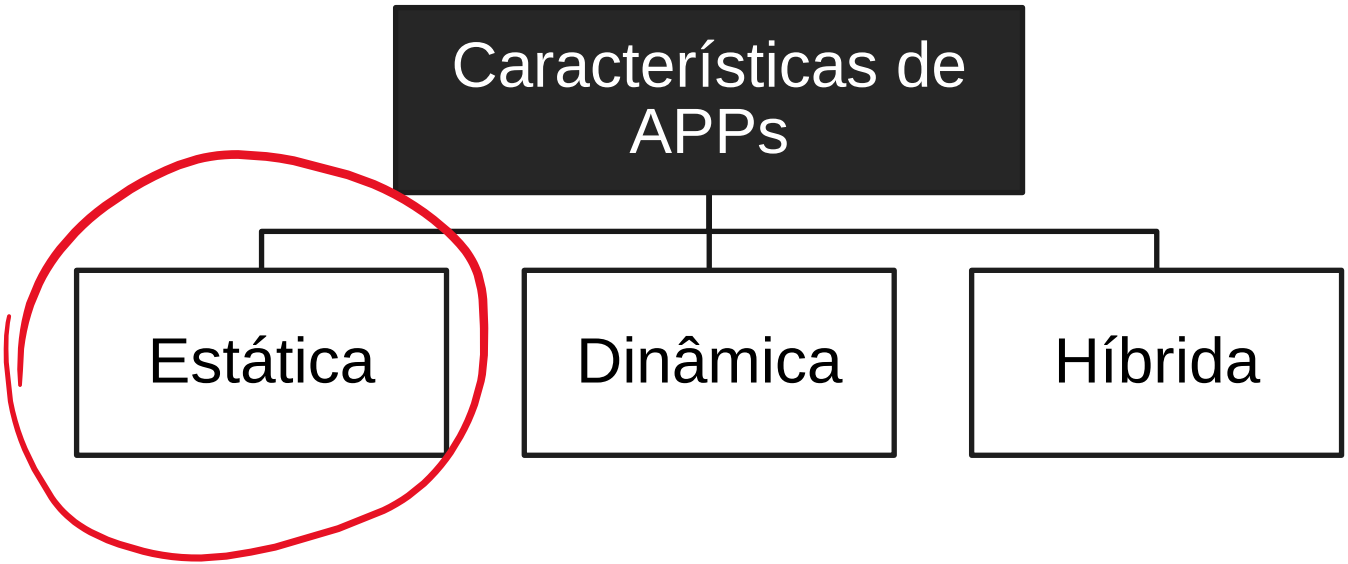
- Mais de 70% dos *smartphones* usam Android
- Alvo preferido de criminosos cibernéticos

Contexto

Detecção de *malware*



Motivação



Objetivo

Avaliar ferramentas de extração de características estáticas de APKs

Metodologia — etapas

Levantamento de ferramentas

Metodologia — etapas

Levantamento de ferramentas

Avaliação de admissibilidade das ferramentas

Metodologia — etapas

Levantamento de ferramentas

Avaliação de admissibilidade das ferramentas

Seleção de APKs

Metodologia — etapas

Levantamento de ferramentas

Avaliação de admissibilidade das ferramentas

Seleção de APKs

Avaliação das ferramentas

Metodologia – ferramentas selecionadas

Ferramenta	Entradas	Saídas
Androguard	Arquivos .dex e .apk	Características estáticas/arquivos do APK
PScout	Arquivo de manifesto	Permissões
PHP APK Parser	Arquivos .apk	Características estáticas/arquivos do APK
AndroParse		Características estáticas
Mobile Audit		
Android Decompiler		Arquivos do APK
Apktool		

Metodologia – aplicativos selecionados

Benignos

Aplicativo	Tamanho (em bytes)	API
Cartola FC	34.424.77	29
Instagram	40.166.591	30
IPTV	22.460.779	28
Spotify	30.940.271	29
WhatsApp	33.727.503	29

Metodologia – aplicativos selecionados

Maliciosos

Aplicativo	Tamanho (em bytes)	API
Tracking Covid-19	3.172.731	29
Covid19 Symptom Tracker	1.849.005	28
Covid-RD	52.267.255	28
Covid-19	7.821.886	28
Corona Help	25.148.214	29

Resultados – ferramentas de extração

Aplicativos benignos

Ferramenta	Permissões	Intents	Comp. do APP
Androguard	144	292	934
PHP APK Parser	140	74	565
Mobile Audit	144	*	846
PScout	9	0	0

Apenas Androguard foi capaz de obter dados de API e opcode

Resultados – ferramentas de extração

Aplicativos maliciosos

Ferramenta	Permissões	Intents	Comp. do APP
Androguard	49	53	91
PHP APK Parser	39	13	46
Mobile Audit	33	*	91
PScout	0	0	0

Resultados – ferramentas de eng. reversa

Apktool: extraiu os arquivos de todos os APKs conforme esperado

Android Decompiler: arquivos dos APKs não obtidos

Considerações finais

- Androguard: melhores resultados
- Mobile Audit e PHP APK Parser: bons resultados para permissões
- Apktool execução a contento
- Android Decompiler: insatisfatório

Trabalhos futuros

- Maior número de ferramentas e APKs
- Comparação qualitativa e quantitativa
- Construção de *dataset*

UFAM

ICOMP
Instituto de Computação

unipampa
Universidade Federal do Pampa

Obrigado!

https://cutt.ly/GROqXmI

pontes@icomp.ufam.edu.br