MICHEL LUTZ

O custo da compatibilidade

MOBILE 2026*

e a nova era de exploits com IA

TDC FLORIPA - JULHO 2026

WWW.MICHELTLUTZ.ME

TABELA DE-CONTEÚDO

OBRIGADO POR PARTICIPAR

SOBRE*

Arquiteto de Soluções Mobile e Pré-Vendas na AI/R Company

Arquiteto de Soluções Mobile e Pré-Vendas na AI/R Company. Com 18 anos de experiência em engenharia de software, atuo na intersecção entre arquitetura mobile de alta escala, inteligência artificial e viabilidade de negócios.

- MBA em BI, Marketing Digital e Estratégia Data Driven
- MBA em Tecnologia para Negócios: AI, Data Science e Big Data.

MICHEL ANDERSON LUTZ TEIXEIRA

01.

VISÃO GERAL

BRASIL

7º

MAIOR ALVO DE ATAQUES DIGITAIS NO MUNDO

Manter dispositivos legados é um dilema financeiro. O custo de manter market share deve ser pesado contra o risco de brechas cibernéticas.

DOMÍNIO DOS BANKERS

Os dados dos relatórios da Kaspersky **(Securelist Q2 e Q3 2025)** mostram uma escalada na complexidade dos ataques. No terceiro trimestre de **2025**, foram descobertos quase **198 mil pacotes de instalação maliciososfocados em dispositivos mobile.**

A maior ameaça financeira atual atende pelo nome de **Trojans Bancários** (malwares focados em roubar credenciais financeiras e burlar autenticações), com mais de 52 mil novas amostras detectadas apenas no Q3.

Fonte: CNN Brasil / DeepStrike, Fortinet 753,8 bi em 2025

O NÚMERO DE ATAQUES COM TROJANS BANCÁRIOS EM SMARTPHONES AUMENTOU

56%

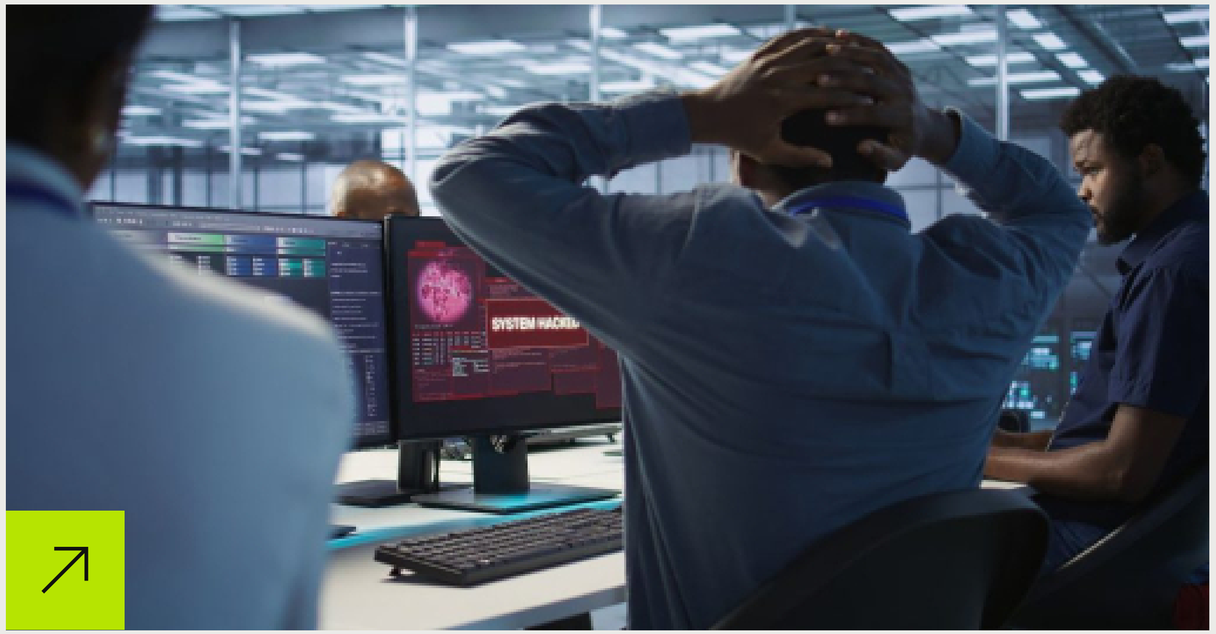
em 2025

O atacante não precisa de zero-day.

A Kaspersky detectou quase 200 mil pacotes maliciosos só no Q3 e mais de **52 mil** eram banking Trojans. No ano, foram 255 mil pacotes únicos de bankers, um salto de 271%.

Fonte: Securelist Q3 2025, Press release +56%

HOJE VAMOS ALÉM DO CHECKLIST E OLHAR PARA DADOS E ARQUITETURA



O custo da retrocompatibilidade

O que muda na engenharia quando exploits conhecidos ganham escala com IA.

*FAMÍLIAS DE MALWARE: MAMONT VS. COPER

Industrialização de exploits conhecidos, **o atacante não precisa de zero-day**

**Banking Trojan: Malware que rouba credenciais ou manipula transações financeiras no device*

MAMONT

Volume de APKs

- ~50–61% do volume de bankers
- Variantes para evadir detecção
- Foco: quantidade de pacotes

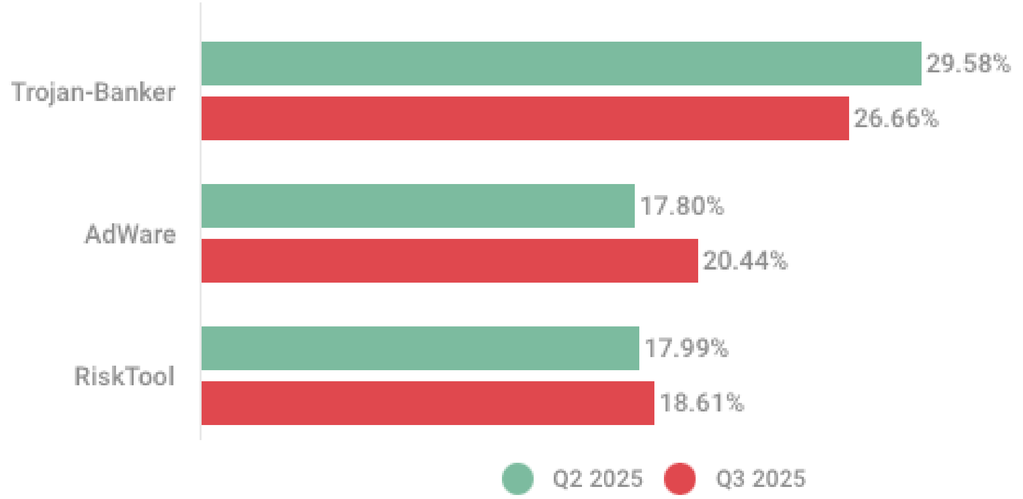
COPER

Usuários atacados

- #1 em usuários efetivamente atacados
- Overlay sobre apps bancários
- WhatsApp/Telegram · sites maliciosos · Google Play

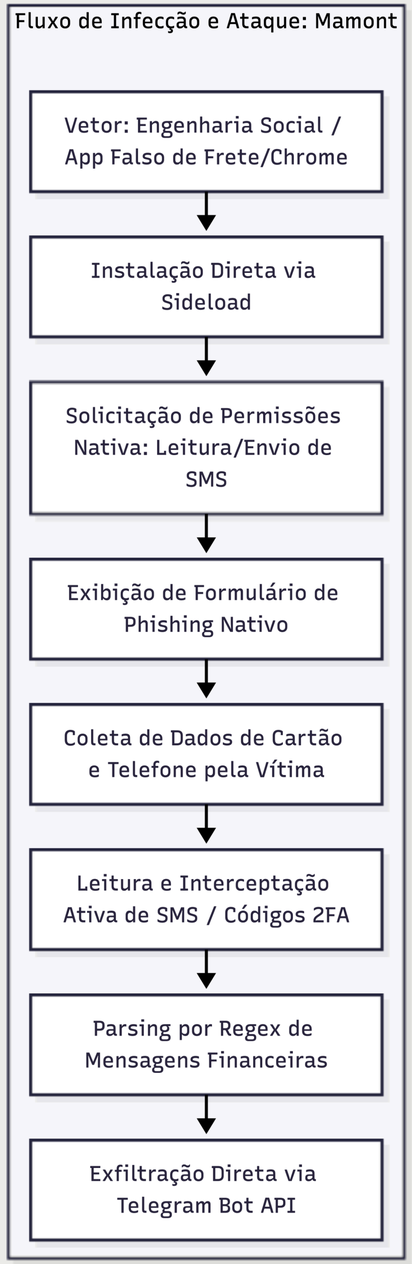
Fonte: Mobile Threat Report 2025, Securelist Q3 2025

FAMÍLIAS DE MALWARE: MAMONT VS. COPER



Fonte: Mobile Threat Report 2025, Securelist Q3 2025

COMO FUNCIONA MAMONT?



*COMO FUNCIONA O COPER?

ETAPA	AÇÃO TÉCNICA	OBJETIVO DO ATACANTE	
1. ENTRADA	Download via Dropper ou Link de Phishing (Sideloading)	Infiltrar o dispositivo sem detecção inicial	Infecção Primária
2. PERSISTÊNCIA & ELEVAÇÃO	Solicitação de ativação do Serviço de Acessibilidade (AccessibilityService)	Garantir controle profundo, auto-permissões e evitar evitar desinstalação	Controle do Sistema
3. CAPTURA DE DADOS	Implementação de WebInjects (Overlay Falsa), Keylogger e Leitura de SMS	Roubar credenciais de login e códigos 2FA de apps bancários	Roubo de Credenciais
4. EXECUÇÃO DE FRAUDE (ODF)	Streaming de Tela (RAT/VNC) e Gestos/ cliques automatizados	Realizar transações financeiras ilegais dentro do app legítimo da vítima	Perda Financeira

O DILEMA DA RETROCOMPATIBILIDADE

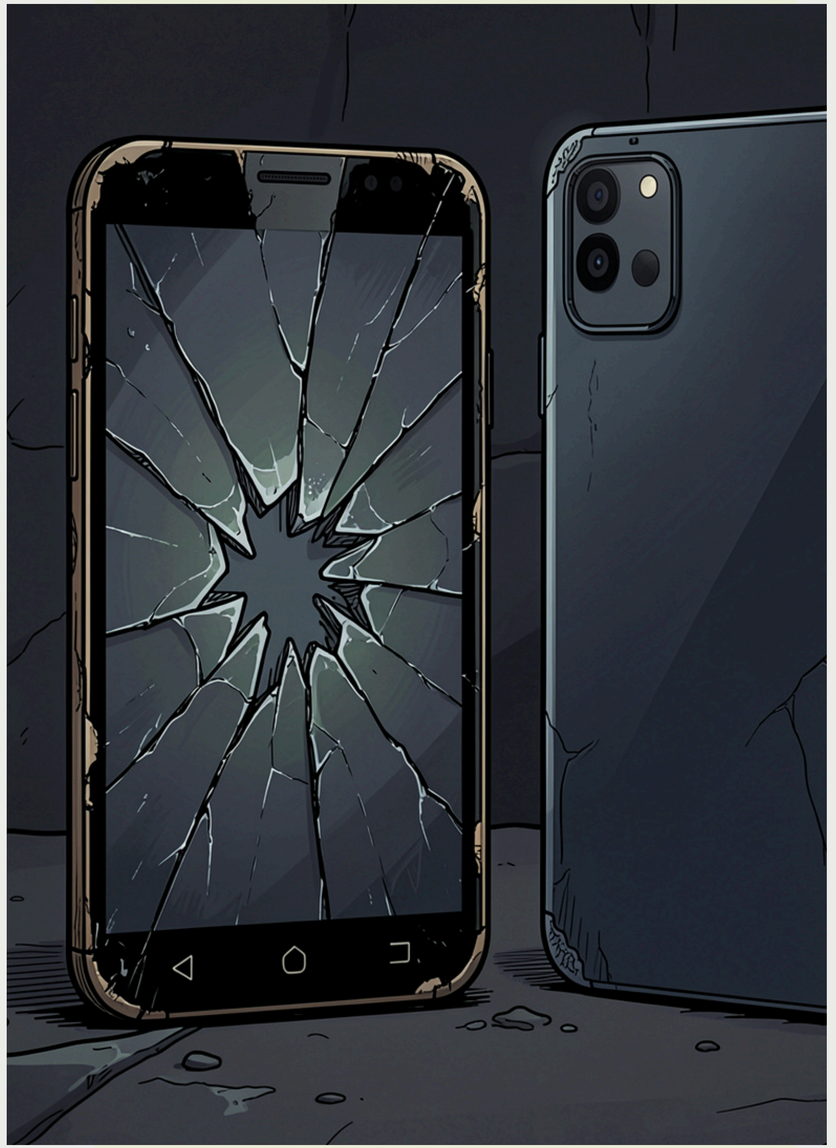
Manter suporte a dispositivos antigos é uma decisão de risco — não apenas de UX.

CVE-2012-6636 ainda eficaz

Uma vulnerabilidade de 2012 continua explorável em 2026. O Android Security Bulletin documenta, mas a adoção de patches é lenta.

Caso Djini: WebView → RCE

Compatibilidade legada se torna dívida de segurança: suportar versões antigas do WebView expõe o app a injeção remota de código.



GENAI OFENSIVA VS. DEFENSIVA

O caso Djini.ai ilustra o ponto central: um LLM acelerou a descoberta de uma JS Bridge vulnerável. A IA amplifica tanto o ataque quanto a defesa — a diferença está na governança humana.

* CASO DJINI.AI EM DETALHE

→ RESILIÊNCIA

01. VETOR

WebView vulnerável em versão legada do Android

02. ACELERAÇÃO

LLM identifica JS Bridge exposta em minutos

03. IMPACTO

Remote Code Injection, execução arbitrária no dispositivo

04. DEFESA

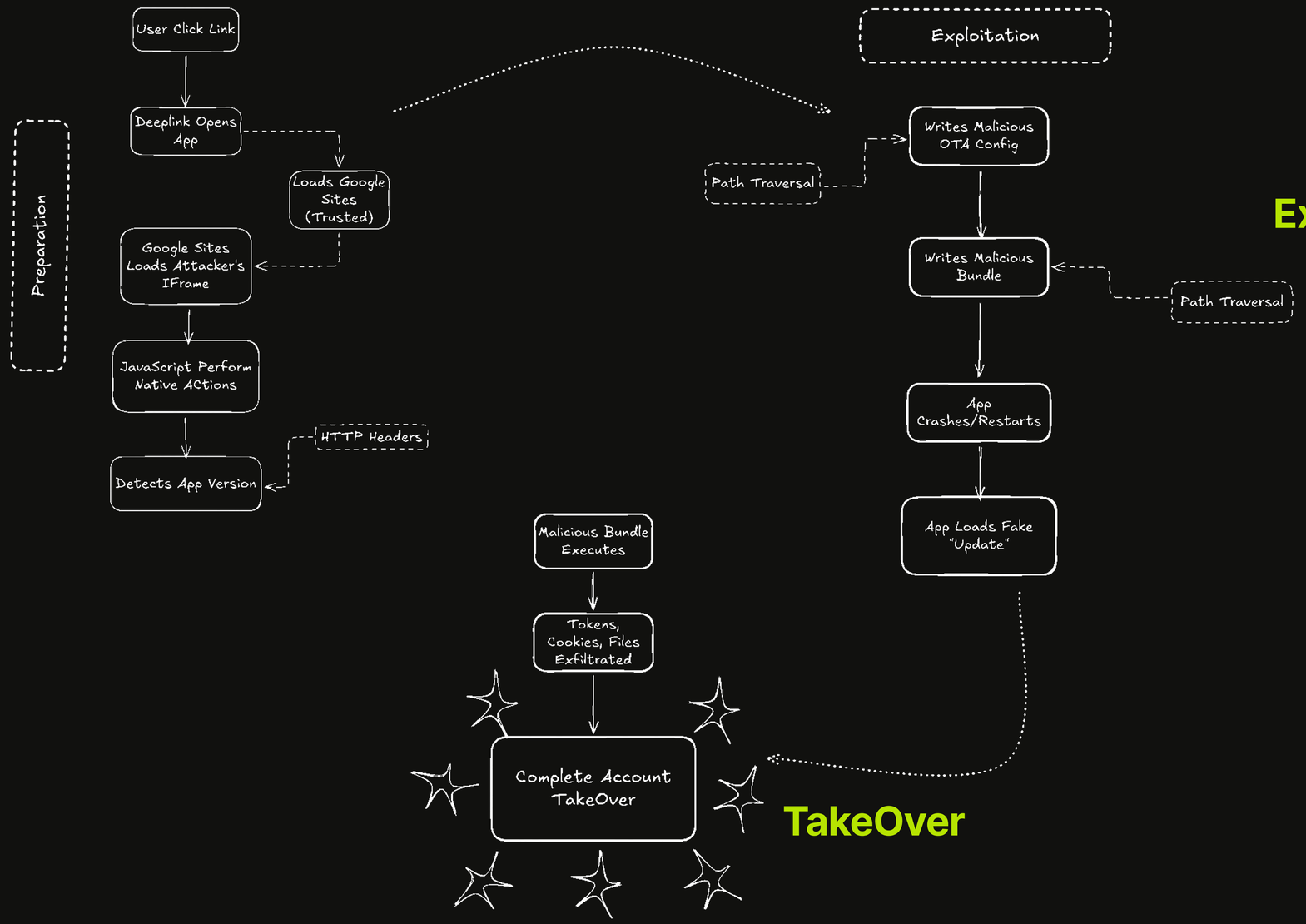
Sunset policy + revisão de bridges com governança humana

As **CVEs** (Common Vulnerabilities and Exposures) são, essencialmente, um dicionário de vulnerabilidades de segurança de software e hardware conhecidas publicamente.

↗

CASO DJINI.AI EM DETALHE

Preparation

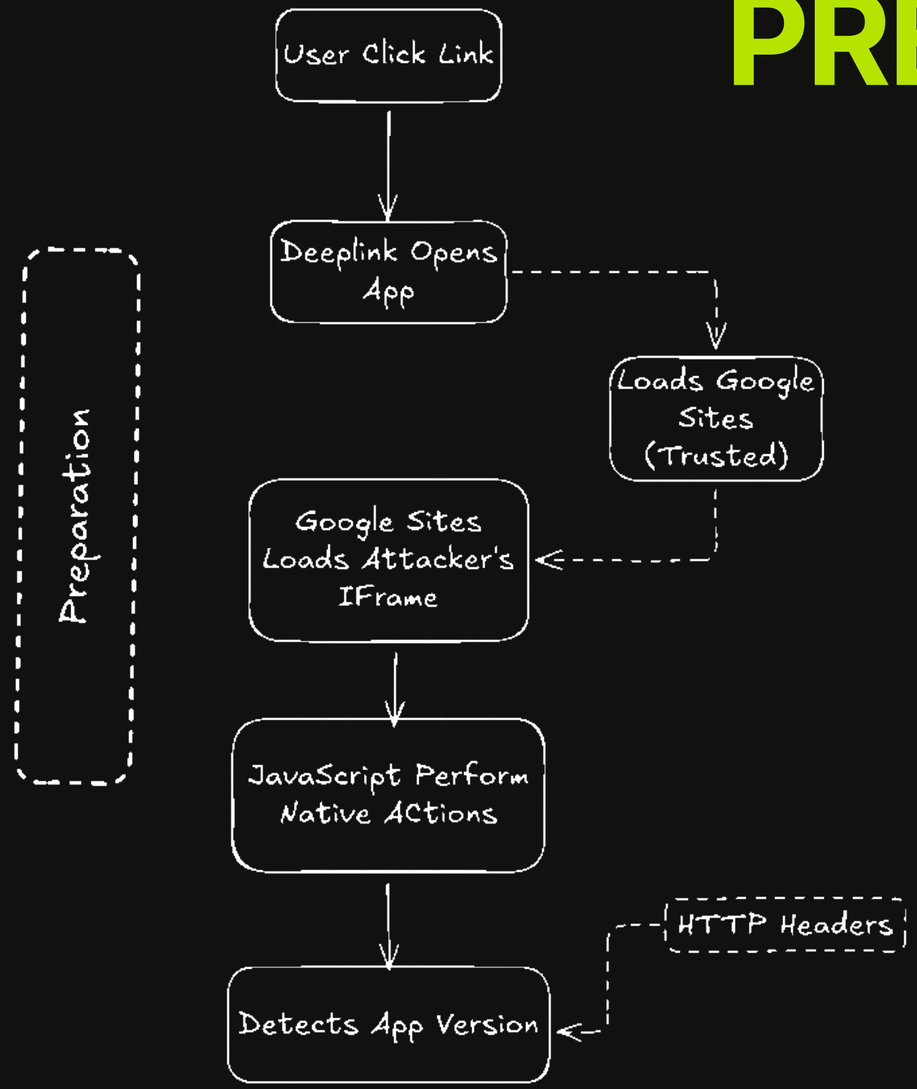


Explotation

TakeOver

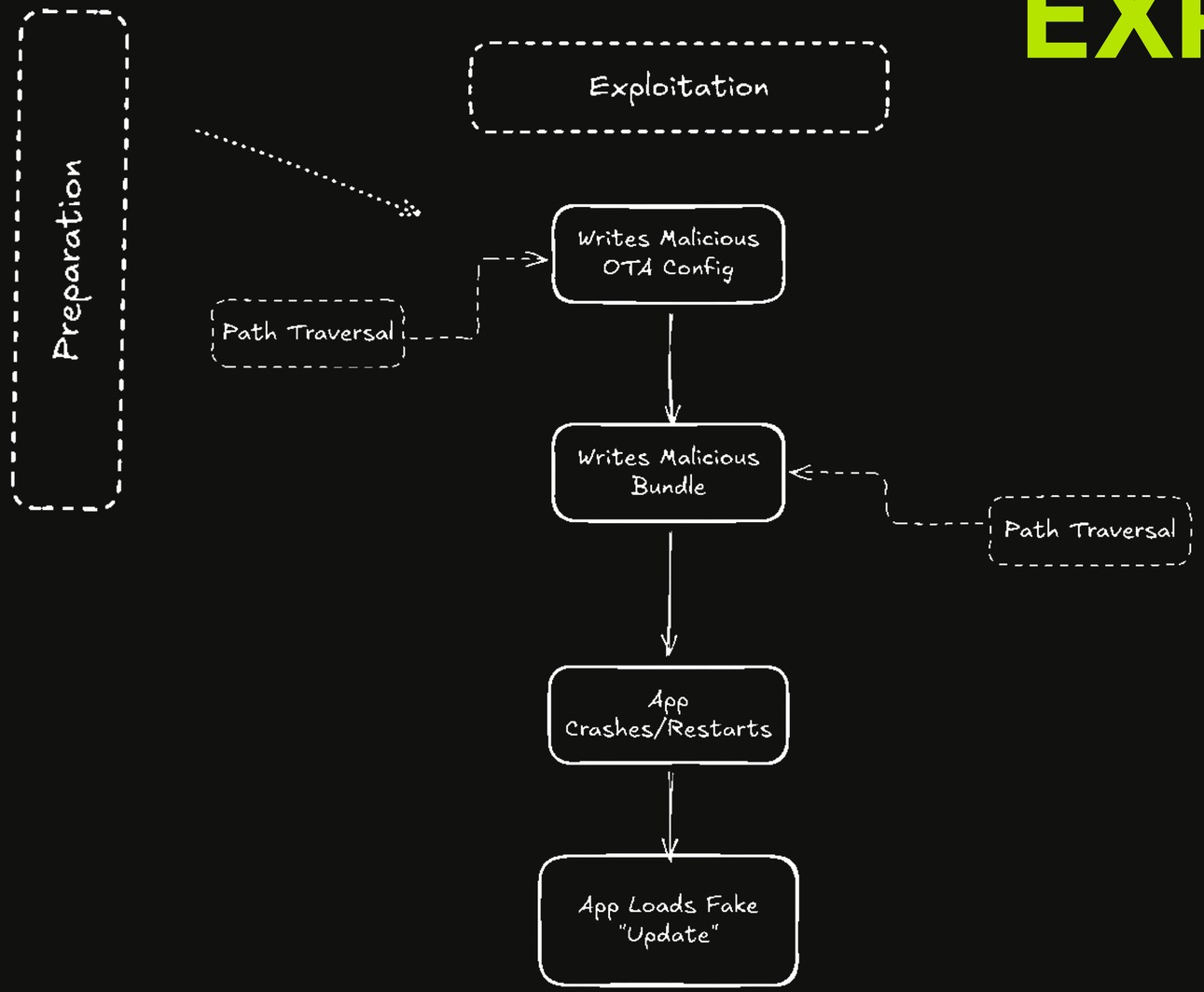
CASO DJINI.AI EM DETALHE

PREPARATION



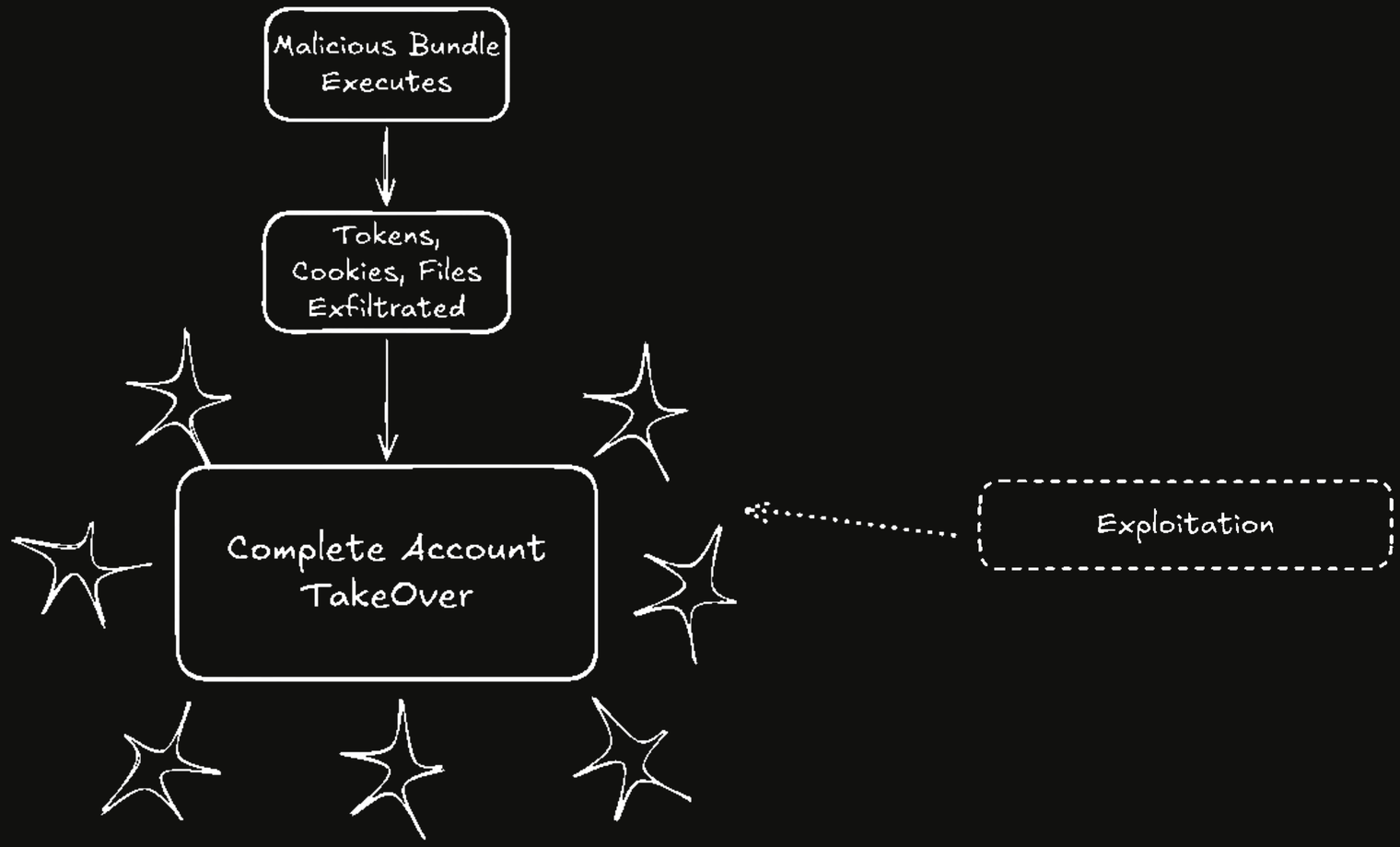
CASO DJINI.AI EM DETALHE

EXPLOITATION

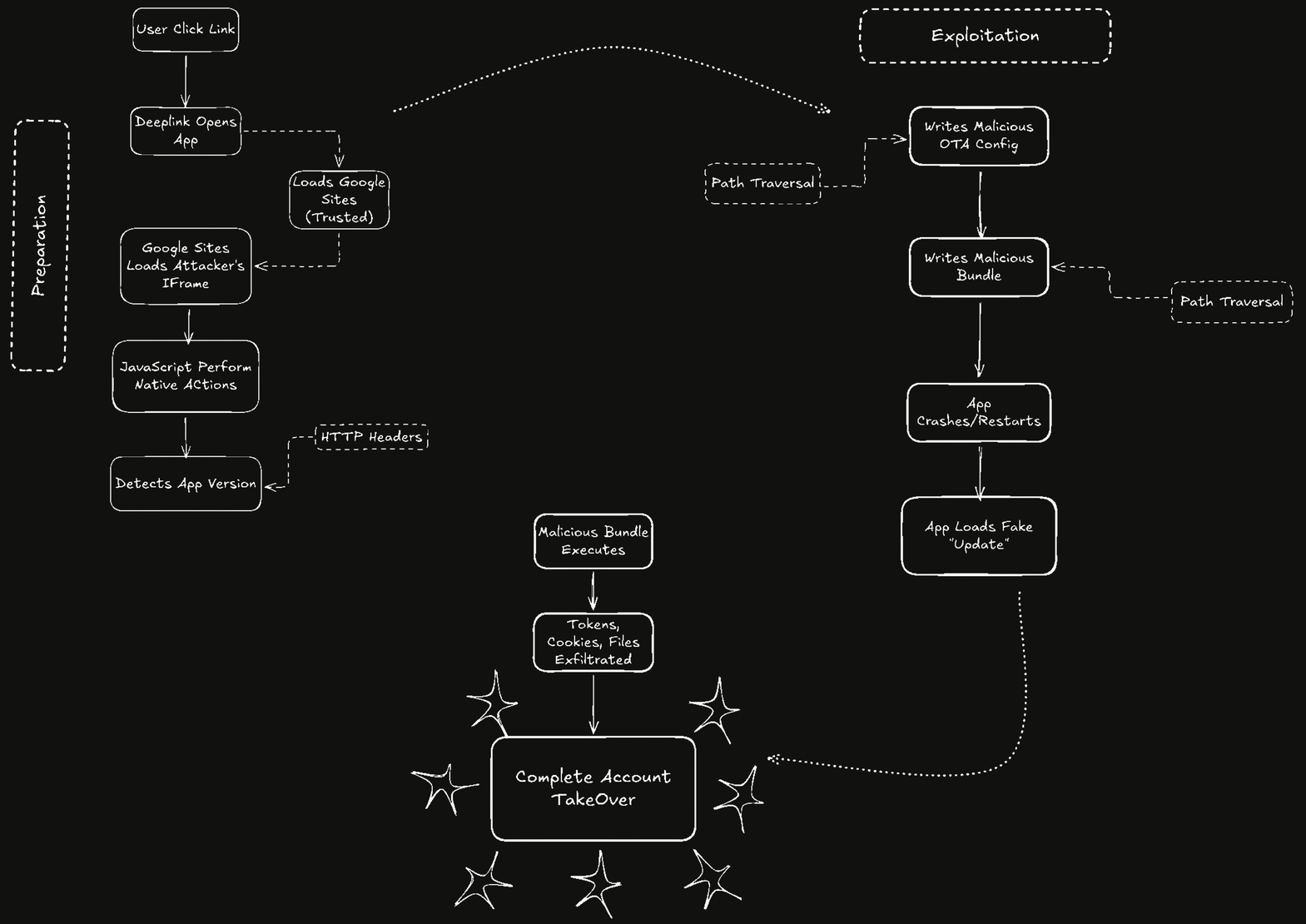


CASO DJINI.AI EM DETALHE

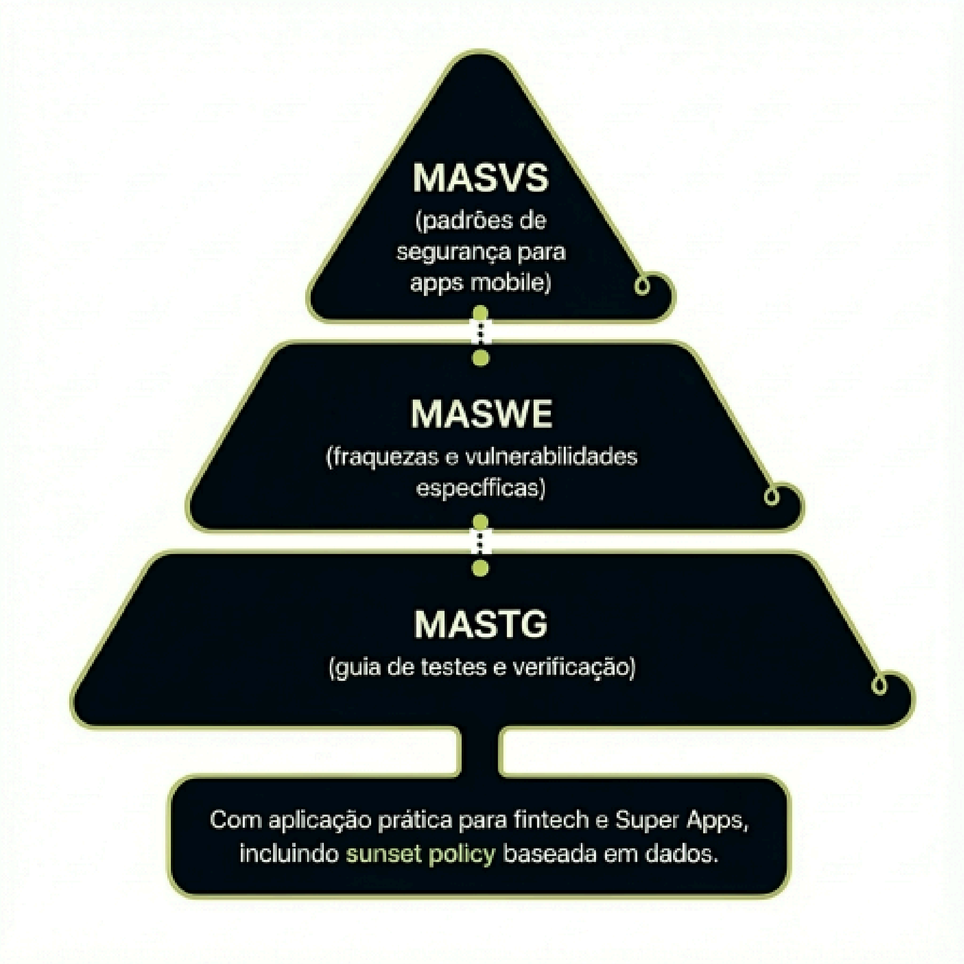
TAKEOVER



CASO DJINI.AI EM DETALHE



FRAMEWORK OWASP MAS



Espinha dorsal da palestra

O framework OWASP MAS estrutura a abordagem em três camadas:

- MASVS — padrões de segurança
- MASWE — catálogo de fraquezas
- MASTG — guia de testes

Com foco em priorização para fintech e Super Apps e política de sunset baseada em dados.

*GESTÃO DE OBSOLESCÊNCIA

→ **RESILIÊNCIA**

As **CVEs** (Common Vulnerabilities and Exposures) são, essencialmente, um dicionário de vulnerabilidades de segurança de software e hardware conhecidas publicamente.

01. SUNSET DATA-DRIVEN

Decisões de descontinuação baseadas em telemetria real e severidade de **CVEs**, não em opinião.

02. DÉBITO COM PRAZO

Cada linha de código legado é um passivo. Defina janelas de suporte atreladas à segurança.

03. RESILIÊNCIA ATIVA

Implemente camadas de segurança proativas para proteger o que ainda não pode ser migrado.

* QUANDO DIZER ADEUS AO LEGADO?

A decisão de descontinuar o suporte a uma versão antiga de um sistema operacional ou dispositivo é difícil.

Ela envolve ponderar o impacto no market share com os riscos de segurança e os custos de manutenção.

→ **3 PONTOS PARA APOIAR A DECISÃO**

01.

ANÁLISE DE RISCO

O SO antigo suporta isolamento de hardware (TEE)? Se não, o risco é inaceitável em 2026.

02.

IMPACTO DE MARKET SHARE

Menos de 2% da base ativa? Hora de converter usuários para o novo ecossistema.

03.

CUSTO DE MANUTENÇÃO

O tempo gasto em retro-compatibilidade está matando o lançamento de features de IA?

DORA METRICS PARA MOBILE

01. DEPLOYMENT FREQUENCY

Frequência de código "Production-Ready" no merge principal.

02. LEAD TIME FOR CHANGES

Do commit ao binário disponível em track de testes.

03. CHANGE FAILURE RATE

Sessões livres de crash nas primeiras 24h pós-release.

04. TIME TO RESTORE

Tempo para desligar features via Remote Config ou rollback.

FONTES DE DADOS PARA DECISÃO

GLOSSÁRIO

MAU (Monthly Active Users)
DAU (Daily Active Users)

01. TELEMETRIA DE USO

Onde: Firebase Analytics, Amplitude ou Mixpanel.

Extraia o volume de usuários ativos (MAU/DAU) segmentado por OS Versione Device Model.

02. SAÚDE E SEGURANÇA

Onde: Crashlytics e Scanners de Vulnerabilidade.

Monitore a taxa de sessões sem crash (Crash-free) e o número de CVEs abertas para APIs antigas.

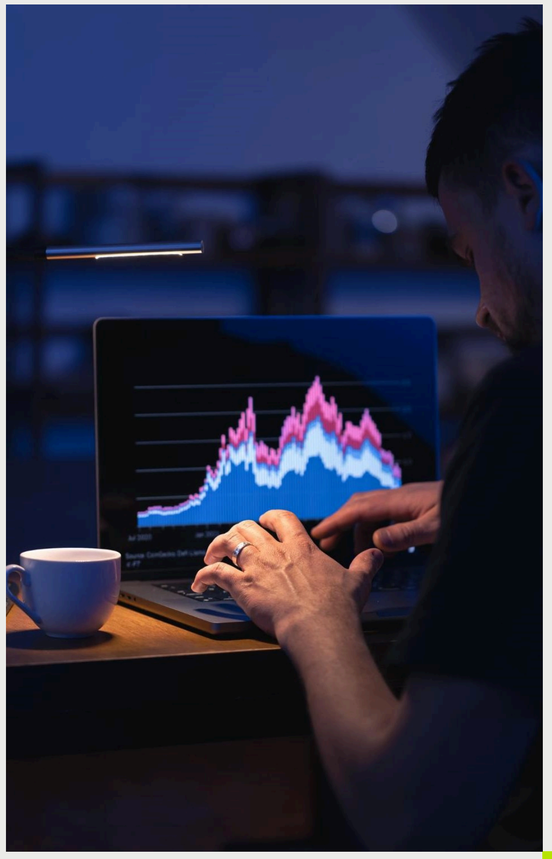
03. EFICIÊNCIA DE TIME

Onde: Jira e Métricas DORA.

Mensure o Lead Time gasto apenas em bugs de retrocompatibilidade vs. novas features.

RISCOS vs TOMADA DE DECISÃO

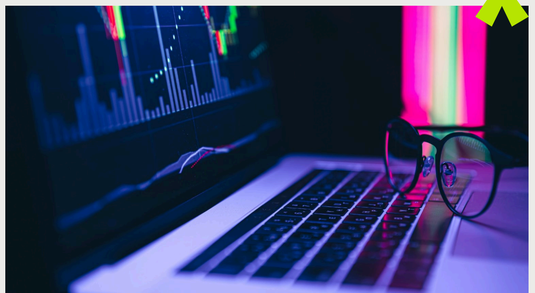
CRITÉRIO	MANTER LEGADO	MIGRAÇÃO/SUNSET
Market Share	Retém usuários em dispositivos antigos	Risco de churn de baixa renda
Segurança	Vulnerável a ataques de IA em APIs velhas	Postura de Resiliência Cibernética
Custo de Engenharia	Alto (Manutenção e QA fragmentado)	Foco em inovação e novas APIs
Risco de Compliance	Passível de incidentes e multas	Alinhado com normas 2026



A LINGUAGEM DO BOARD

SUBSTITUA O TÉCNICO PELO ESTRATÉGICO:

"Não estamos abandonando usuários; estamos eliminando um canal onde o risco de fraude assistida por IA é maior que o lucro gerado."
"80% do nosso esforço de suporte hoje serve a apenas 2% da nossa base de usuários legada."



REFERÊNCIAS*

- *Gartner (2023): Gartner Says More Than 80 Percent of Enterprises Will Have Used Generative AI APIs or Deployed Generative AI-Enabled Applications by 2026.*
- *PwC Brasil: Digital Trust Insights 2026.*
- *FAIR Institute: Factor Analysis of Information Risk.*
- *OWASP MAS (Mobile Application Security)*
- *DORA (DevOps Research and Assessment): The ROI of AI-assisted Software Development (2026).*
- *Google Cloud / DORA: DORA Metrics Guide.*
- *Mobile 2026: O Preço da Compatibilidade e o Fator Humano na Segurança*
- *Kaspersky Securelist — Q2 2025 Mobile Statistics*
- *Kaspersky Securelist — Q3 2025 Mobile Statistics*
- *Kaspersky — Mobile Threat Report 2025*
- *Kaspersky — Press release: banker attacks +56% em 2025*
- *Fortinet FortiGuard — Cenário Global de Ameaças 2026 (dados 2025)*
- *DeepStrike / CNN Brasil — 7º maior alvo global (1º semestre 2025)*
- *Securelist Brazil — Panorama mobile 2025 (PT-BR)*
- *Malwarebytes — Press release (estudo completo)*

THANK YOU

Meu site e slides no menu Palestras