MISP to intelligence mobile protection

TLP:CLEAR

WHOAMI?

Meu nome é Gabriel Lucas. **Analista de Inteligência de Ameaças no Banco Inter**,Atuação direta nas áreas de **Cyber Intelligence** e **Fraud Intelligence**

Formado em **Redes de Computadores** e pós-gradudo em **Defesa Cibernética**, Atualmente cursando uma pós-graduação em **Threat Intelligence**,

Algumas certificações e diversos cursos ligados a **CSIRT** e **Defesa Cibernética**,

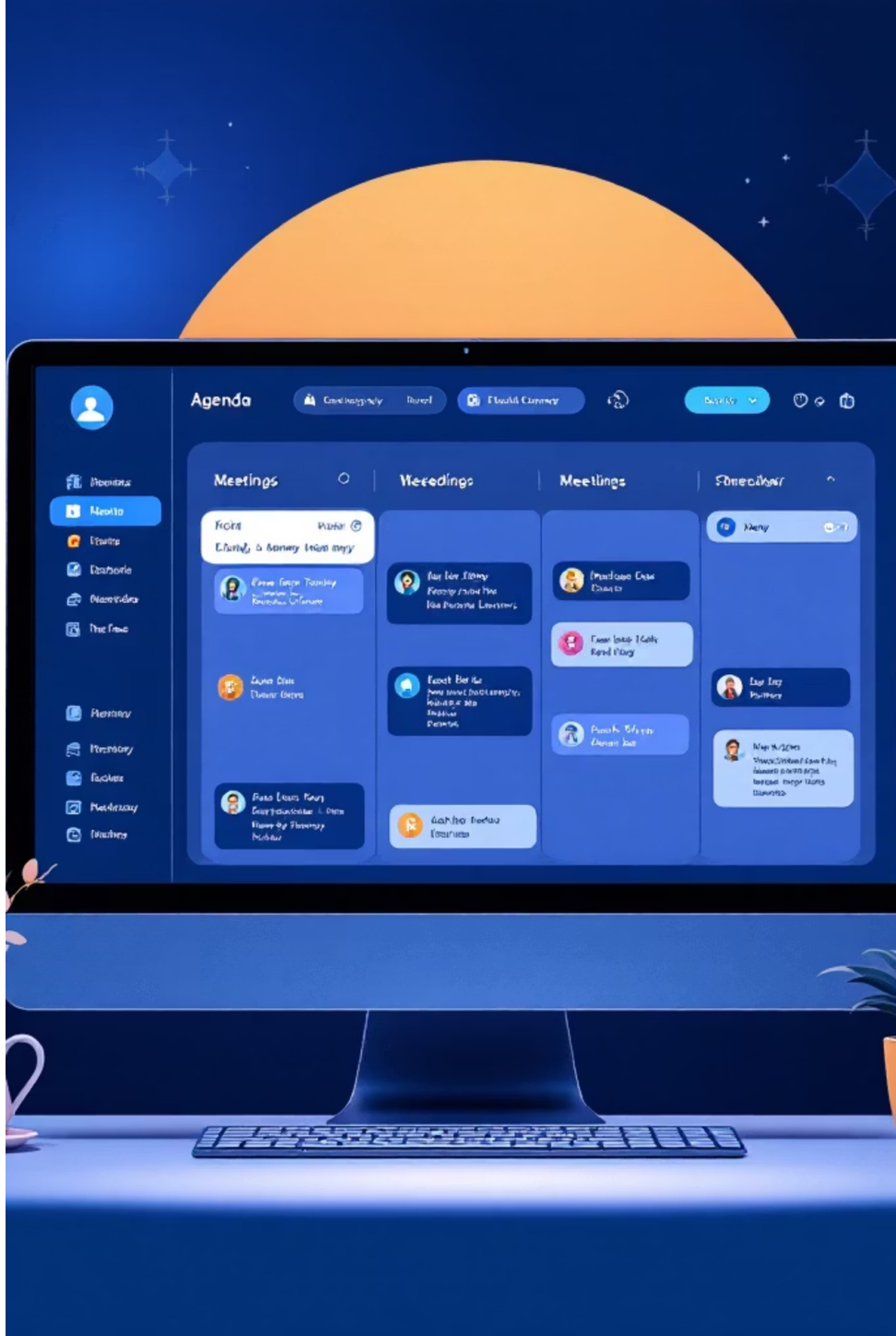
Aspirante a criador de conteúdo sobre segurança cibernética e palestrante quando possível. 😎

TLP:CLEAR

Agenda

- Disclaimer
- Introdução e contexto geral
- Objetivo
- Desafios x Soluções
- RAT
- Inteligência direcionada com MISP
- Possibilidades
- Agradecimentos

TLP:CLEAR



Disclaimer

⚠ As opiniões e informações apresentadas nesta palestra refletem exclusivamente minha visão pessoal e profissional, com base em experiências práticas e estudos técnicos.

⚠ Nenhuma informação aqui compartilhada deve ser interpretada como posicionamento oficial da empresa ou como recomendação definitiva de segurança.

⚠ O conteúdo é voltado para fins educacionais e estratégicos, com o objetivo de fomentar discussões sobre segurança mobile, inteligência contra ameaças e prevenção a fraudes.

TLP:CLEAR

MISP Além do tradicional

Network activity **NULL:** raptorit.rmmservice.com
domain

Network activity **NULL:** 82.29.54.36
ip-dst

Payload delivery **filename:** payment slip005621.exe
filename

MISP
Threat Sharing

Payload delivery sha256 277730f312b07a3f7b5565b6b1afd037f977c89cd906ac0ba5743f9d4fc376d6

- Plataforma open-source para gestão e compartilhamento de Threat Intelligence.
- Projetado para colaborar e automatizar a detecção e resposta a ameaças.
- Normalmente aplicado a ameaças convencionais (infra, endpoints, redes).

TLP:CLEAR

Gerando inteligência para fortalecer a defesa mobile com MISP

Nosso principal objetivo com este projeto é gerar inteligência técnica e acionável para o time de segurança mobile.Assim como outras áreas da cibersegurança já se beneficiam do uso de plataformas como o MISP, queremos trazer essa mesma maturidade para o universo mobile.

Centralização da inteligência

Reunir dados de diversas fontes em um único repositório, garantindo rastreabilidade, histórico e contexto.

Automação

Fluxo para minimizar o tempo entre a detecção de uma ameaça e sua mitigação, integrando diretamente com soluções de Mobile Threat Defense.

Análise técnica mobile

Não apenas listar hashes ou domínios, mas sim entender campanhas, relacionar com APTs, e entregar insights úteis ao time mobile.

Capacidade de resposta

Disponibilização de inteligência que capacita o MTD a decisões mais assertivas.

Ameaças móveis em ascensão

TLP:CLEAR

Análise de padrões

Em 2025 a Malwarebytes identificou aumento de 151% nas ameaças Android no primeiro semestre do ano

Alto Impacto

Acesso direto a dados sensíveis, apps bancários e MFA.

Vetores

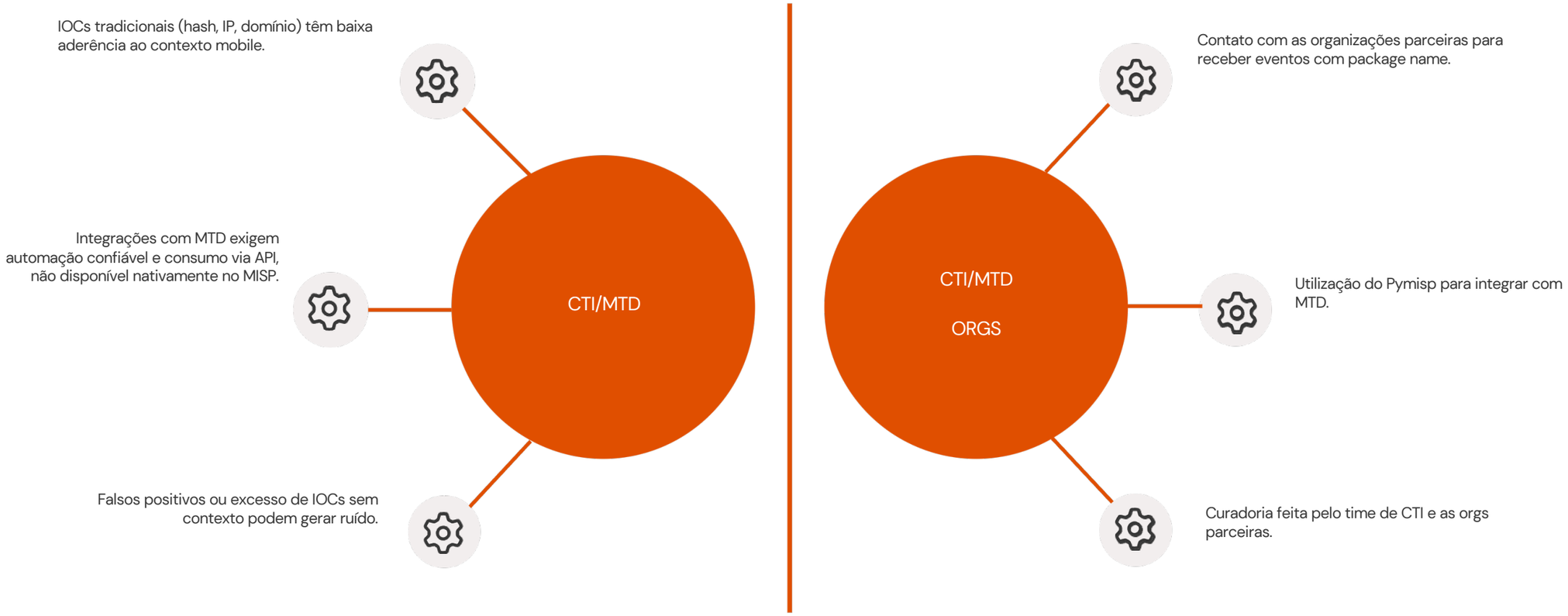
Phishing por SMS/WhatsApp, apps falsos e exploits zero-day

Ameaças Globais

APTs móveis ganhando espaço (ex: Pegasus, Hermit, Android RATs)

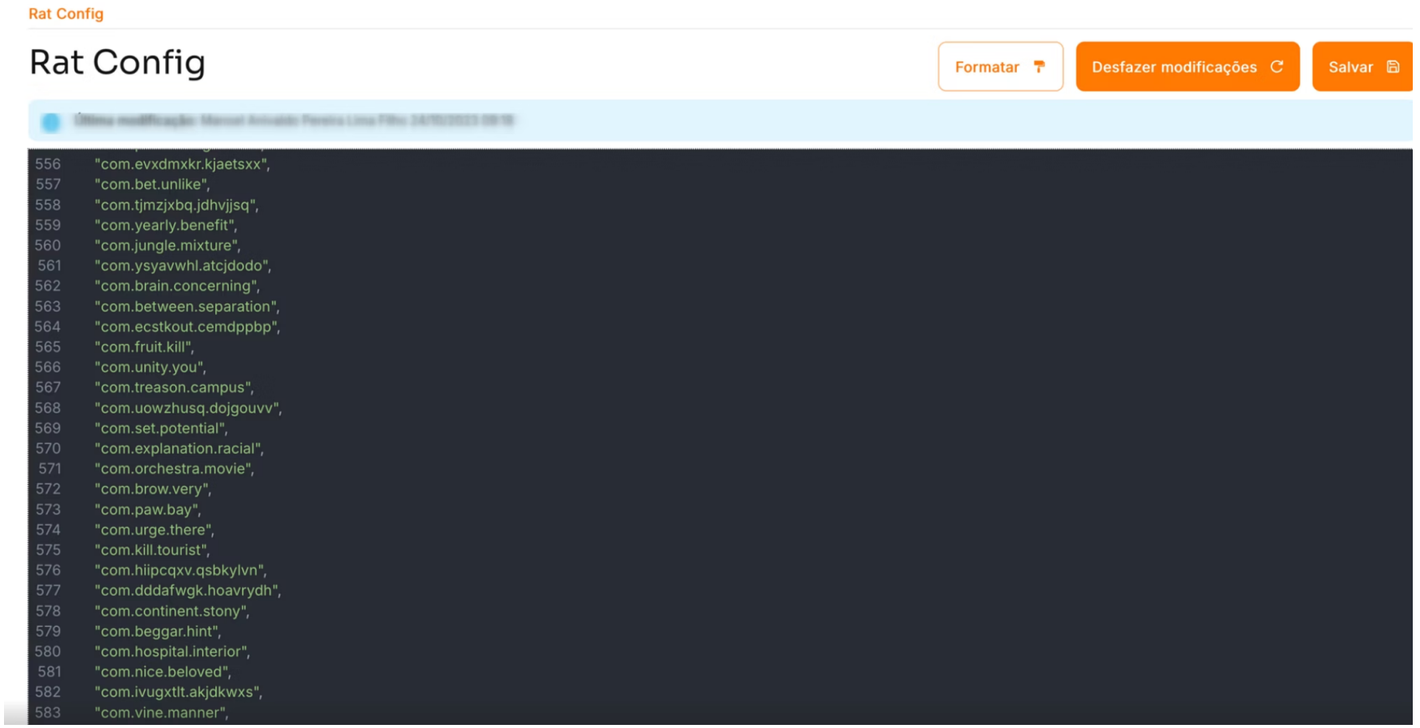
Nos últimos anos, as ameaças móveis deixaram de ser uma preocupação secundária. Vimos um aumento superior a 400% em malwares voltados para dispositivos móveis. E não estamos falando apenas de apps espiões genéricos, mas sim de campanhas avançadas como Pegasus, Hermit e Android RATs.

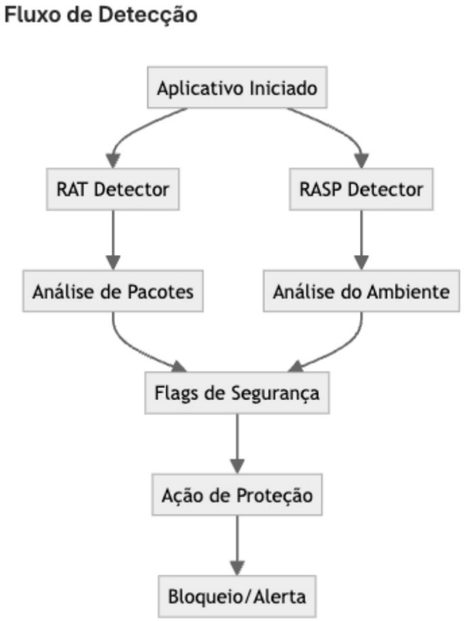
Desafios x Soluções



TLP:CLEAR

Runtime Application Threat





Dois Fluxos de Detecção Serviços de Acessibilidade: Identifica serviços com capacidades e flags suspeitas (ex: capturar tela, interceptar teclas). Classifica como: MALICIOUS: se estiver na blacklist. ACCESSIBILITY_RISK: se for desconhecido e de alto risco.

A RAT config **(Runtime Application Threat) é responsável por detectar e monitorar aplicativos maliciosos e serviços de acessiilidade suspeitos em tempo de execução. Ele funciona como uma camada de proteção que analisa continuamente os pacotes instalados no dispositivo e os serviços de acessibilidade ativos.**

TLP:CLEAR

Runtime Application Threat

Recommended queries | Recent queries | Clear | Run

Since 1 hour ago | Chart type: Table

Malicious Apps	Sistema Operacional	Mac Address	Versao App	Dispositivo	App Safe Flags
[br.com.mobcriative.loteria]	ANDROID	3[redacted]	14.0.2	SM-G781B	[MALICIOUS:br.com.mobcriative.loteria, TIMESTAMP:1753470381945]
[com.shuyi.csdj]	ANDROID	a[redacted]	14.0.2	SM-A156M	[MALICIOUS:com.shuyi.csdj, TIMESTAMP:1753470382646]
[org.yns.okqxe]	ANDROID	2[redacted]	14.0.2	SM-A346M	[MALICIOUS:org.yns.okqxe, TIMESTAMP:1753470382344]
[com.candypop.tapmelt, com.driver.market, com.enj.video, com.entertainment.com.unity.template.LudoWar, com.fais.flower]	ANDROID	7[redacted]	13.7.4	SM-A057M	[MALICIOUS:com.candypop.tapmelt|com.driver.market|com.enj.video|com.entertainment.c
[com.app.challengeextremenumbersGame]	ANDROID	f[redacted]	13.7.6	SM-A366E	[MALICIOUS:com.app.challengeextremenumbersGame, TIMESTAMP:1753470382249]
[com.arfa.catchangpao, com.scqt.StarCircleQuest, com.wispeos.cotetre, spinwin.vegasdream.winnersquest]	ANDROID	0[redacted]	14.0.2	24117RN76L	[MALICIOUS:com.arfa.catchangpao|com.scqt.StarCircleQuest|com.wispeos.cotetre|spinwi
[com.MyBestHindiShayari]	ANDROID	f[redacted]	14.0.2	moto g84 5G	[MALICIOUS:com.MyBestHindiShayari, TIMESTAMP:1753470382697]
[com.lopet.numberninja]	ANDROID	a[redacted]	14.0.2	SM-A346M	[MALICIOUS:com.lopet.numberninja, TIMESTAMP:1753470374307]
[com.ac.askchat, com.implizn.plutarh]	ANDROID	b[redacted]	14.0.1	SM-A145M	[MALICIOUS:com.ac.askchat|com.implizn.plutarh, TIMESTAMP:1753470381148]
[com.ac.askchat, com.implizn.plutarh]	ANDROID	b[redacted]	14.0.1	SM-A145M	[MALICIOUS:com.ac.askchat|com.implizn.plutarh, TIMESTAMP:1753470381148]
[com.joskip.goodnewsbible]	ANDROID	d[redacted]	14.0.2	2201117TG	[MALICIOUS:com.joskip.goodnewsbible, TIMESTAMP:1753470381994]
[com.pgdemo, com.wofi3.dfk4alfadsf]	ANDROID	b[redacted]	14.0.2	SM-A115M	[MALICIOUS:com.pgdemo|com.wofi3.dfk4alfadsf, TIMESTAMP:1753470382160]
[com.arappspro.reda_talyani_arap]	ANDROID	2[redacted]	14.0.2	moto g22	[MALICIOUS:com.arappspro.reda_talyani_arap, TIMESTAMP:1753470380862]
[com.micredit.in]	ANDROID	9[redacted]	14.0.2	Redmi Note 7	[MALICIOUS:com.micredit.in, TIMESTAMP:1753470383372]
[com.albarooon.app56]	ANDROID	9[redacted]	14.0.2	23100RN82L	[MALICIOUS:com.albarooon.app56, TIMESTAMP:1753470380734]

Valor Agregado:

- Proteção em tempo real contra ameaças que escapam de análises estáticas.
- Detecção proativa de RATs, spywares e malwares bancários.
- Resiliência offline com cache inteligente.
- Privacidade preservada: coleta apenas metadados, sem acessar conteúdo dos apps.
- Baixo impacto de performance, com execução assíncrona e otimizações de cache.

Inteligência Direcionada com MISP

Integração MISP → MTD via API e PyMISP

```python
from pymisp import PyMISP
misp = PyMISP(url, key, ssl=False)
attrs = misp.search(controller='attributes', type='package-name', includeEventTags=False)
```

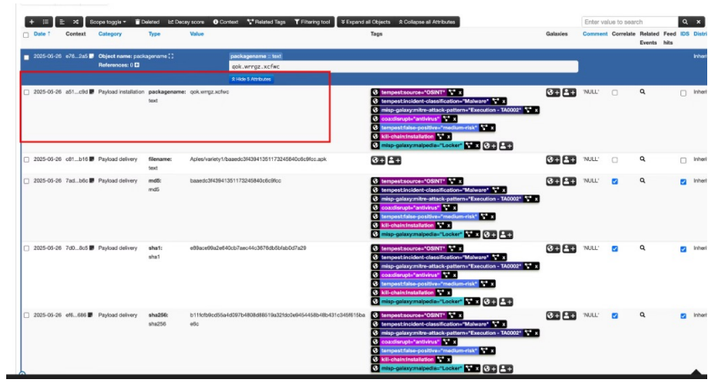
```python
for attr in attrs:
    ev = misp.get_event(attr['event_id'])
    tags = ev['Event']['Tag']
    # extrair campanha, APT ou contexto
```

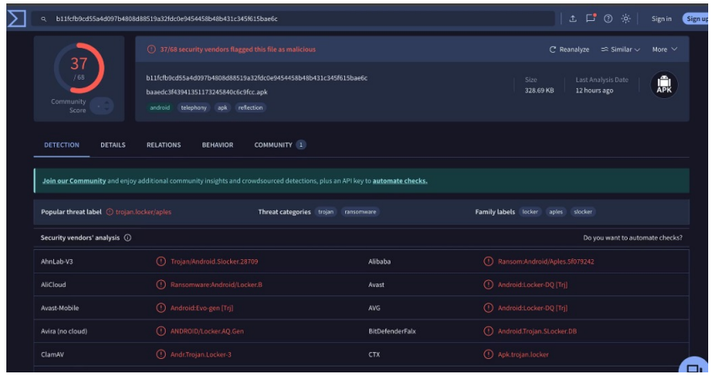
Para identificar campanhas, o PyMISP permite obter atributos vinculados a um evento e seus metadados:

O MISP pode integrar e compartilhar inteligência direcionada, especialmente utilizando PyMISP, e filtrando por ***package names*** recebidos de parceiros confiáveis.

TLP:CLEAR

Inteligência Direcionada com MISP

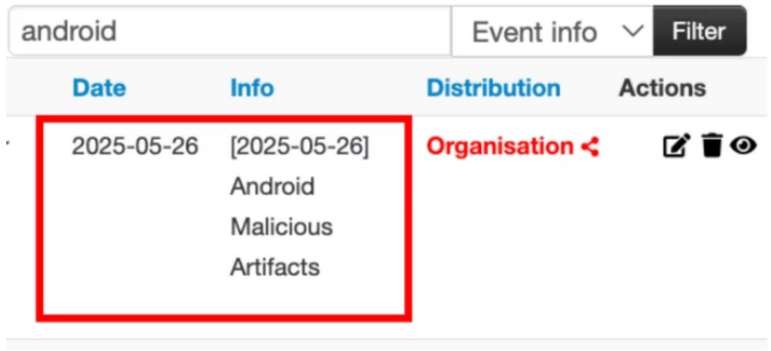




Observação: Package names (como `com.company.appname`) são identificadores únicos e persistentes do aplicativo, independente da versão. Eles funcionam como uma "impressão digital" estável do app. **(Package names seriam equivalentes aos "Tools" da pirâmide da dor)**

TLP:CLEAR

Inteligência Direcionada com MISP

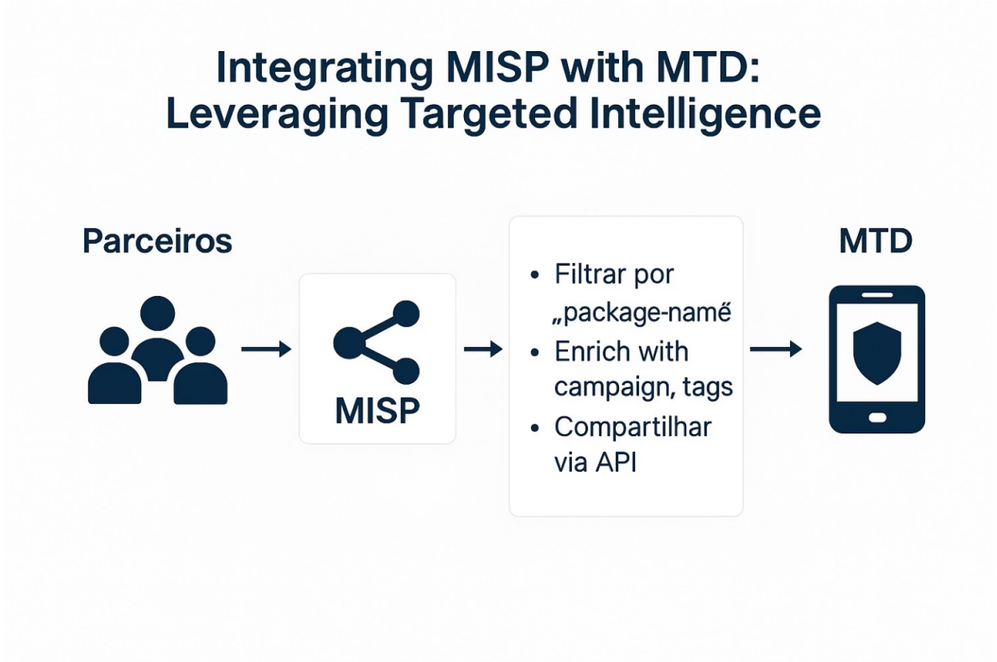



```
[Parceiros] → MISP ← PyMISP (filtra 'package name')
   ↓ extrai campanha/contexto
   ↓ compartilha via API
[MTD recebe IOCs móveis prontos para ação]
```

- Busca no MISP apenas os IOCs do tipo `package-name` (indicadores de apps maliciosos móveis);
- Enriquece com metadados como campanha e nível de ameaça;
- Compartilha automaticamente com sua solução de MTD via API.

TLP:CLEAR

Inteligência Direcionada com MISP



CTI COM MISP GERANDO VALOR PARA ORGANIZAÇÃO.

Aumento de efetividade esperada de 60% de precisão nos bloqueios em MTD, por usar IOCs mais específicos (ex: `package name`, contexto de campanha)

TLP:CLEAR

Possibilidades


inter

Evite fraudes no seu celular

Olá, [[${PrimeiroNome}]]!

Você sabe o que é malware? Esse é o nome dado a programas que podem ser instalados em seu dispositivo com o objetivo de acessar dados, espionar o que você faz e até mesmo baixar ou excluir arquivos.

Como um malware é instalado em seu dispositivo?

- Ao baixar aplicativos disponibilizados através de links desconhecidos ou suspeitos;
- Ao permitir que aplicativos acessem mais permissões do que seria necessário, como funções avançadas de controle do dispositivo;
- Ao usar aplicativos bloqueados pela Play Protect no Android.

Como remover um malware?

É importante fazer a redefinição do dispositivo para as configurações de fábrica do aparelho. Para isso, acesse o site oficial do fabricante e siga as orientações necessárias. Depois, será preciso instalar o Super App do Inter e fazer o cadastro do iSafe.

Como se proteger de malwares?

- Mantenha seu sistema operacional sempre atualizado;
- Utilize um antivírus confiável;
- Não clique em links de origem desconhecida;
- Não instale aplicativos de fontes desconhecidas e nem bloqueados pela Play Protect;
- Tenha cuidado ao conceder permissão de acessibilidade a aplicativos.

Esse tipo de **e-mail enviado ao cliente** é uma ação complementar à detecção feita pelo sistema RAT. Ele serve como **canal de comunicação preventiva e educativa**, e agrega valor à segurança mobile de várias formas.

✅ Benefícios estratégicos

- **Reduz suporte técnico**: usuários bem informados resolvem problemas sem acionar canais de atendimento.
- **Fortalece confiança na marca**: mostra que o app está atento à segurança do cliente.
- **Complementa a RAT com ação humana**: enquanto a RAT age no código, o e-mail age na consciência do usuário.

TLP:CLEAR

Possibilidades

Enriquecimento de Inteligência de fraude

- Bloquear ou desviar o fluxo de validação de selfie.
- Invalidar selfies automaticamente se houver apps de clonagem ou manipulação.
- Exigir validação manual em casos de risco elevado.
- Bloquear transações suspeitas (ex: PIX, TED, pagamentos).
- Exigir autenticação reforçada (3FA): biometria + senha + token.
- Restringir valores ou tipos de transação em dispositivos comprometidos.
- Cancelar sessões ativas ao detectar RAT ou spyware.
- Bloquear acesso a funcionalidades sensíveis (ex: extrato, cartão virtual).
- Desabilitar recursos como captura de tela ou gravação de tela.
- Enviar e-mails ou pushs educativos com instruções de segurança.
- Alertar sobre apps instalados sem certificação ou com acessibilidade abusiva.
- Reforçar boas práticas de segurança (atualizações, antivírus, permissões).E ETC...

TLP:CLEAR

Agradeço a atenção de Todos(as)!

O Intelligence Mobile protection é um projeto em andamento e essa apresentação buscou mostrar a arquitetura e resultados preliminares para discussão com a comunidade e feedback.

Gabriel Lucas

Contato do WhatsApp

Disponível para troca de idéias

gabriel.naziazeno@inter.co

Linkedin Gabriel Lucas

TLP:CLEAR