Deteção de Exfiltração de Dados Via WhatsApp

Hugo Moinheiro, 84931
Rafael Amorim, 98197

Índice

01

Segurança do WhatsApp

Integridade de dados

Garante que as mensagens não são alteradas

Criptografia End-to-End

Garante que as mensagens sejam protegidas contra a interceção por terceiros

Verificação em Dois Passos

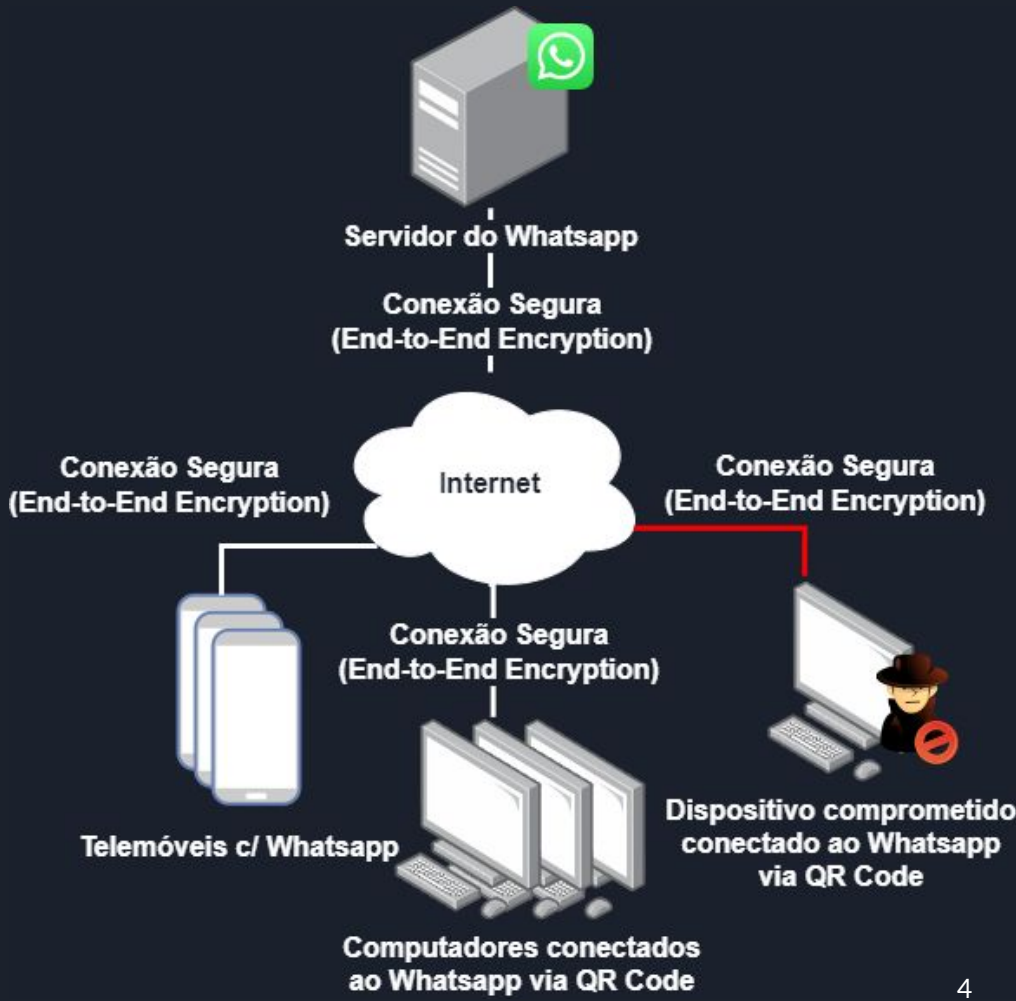
Adiciona outra camada de segurança à sua conta, exigindo uma senha adicional

01

Apesar de Toda a Segurança ...

- Se um dispositivo estiver comprometido pode ser usado para exfiltrar informação confidencial através de qualquer serviço

- Se for usado um serviço frequentemente utilizado para exfiltrar informação pode ser difícil de detetar



02

Cenário real

- Endpoint Detection and Response
- Firewall

Cenário de teste

- Máquina virtual
- Whatsapp web e tráfego normal na Internet

03

Fontes de Dados

- O dados usados para gerar os modelos serão dados reais
- Aquisição de pacotes IP ao longo de 3h + 30min
- Script malicioso para envio de mensagens automaticamente para o WhatsApp

Fontes de Dados

- Criar vários perfis normais

- 2 tipos de Scripts maliciosos:
  - Script "burro”: enviar mensagens longas de forma sequencial
  - Script "inteligente”: tentar replicar o comportamento humano

04

Datasets

- Agregar por fluxos (endereços de origem/destino)

- Para cada fluxo contar:
  - número de pacotes de upload/download
  - total de bytes de upload/download

- Intervalo de periodicidade: 5 segundos

05

Features

- Janelas deslizantes de observação:
  - Largura de 120 intervalos de periodicidade (10 minutos)
  - Deslizamento de 12 intervalos de periodicidade (1 minuto)

05

Features

- Máximos e mínimos
- Percentis (90%, 95%, 98%) e Mediana
- Somatório do total de pacotes e bytes transmitidos
- Média e desvio padrão dos períodos de silêncio e atividade
- Percentagem de pacotes e bytes por fluxos

06

Processos de Observação

- Grande fluxo de dados
- Períodos de silêncio curtos
- Sobreposição de fluxos anormal
- Fluxos em horários anormais

07

Bibliografia

Links relacionados com as ideias obtidas para os problemas de segurança

Ataques :

- https://www.bleepingcomputer.com/news/security/whatsapp-boosts-defense-against-account-takeover-via-malware/
- https://www.bleepingcomputer.com/news/security/whatsapp-voice-message-phishing-emails-push-info-stealing-malware/

Vulnerabilidades:

- https://www.ibm.com/topics/data-exfiltration
- https://nonamesecurity.com/learn/what-is-data-exfiltration/