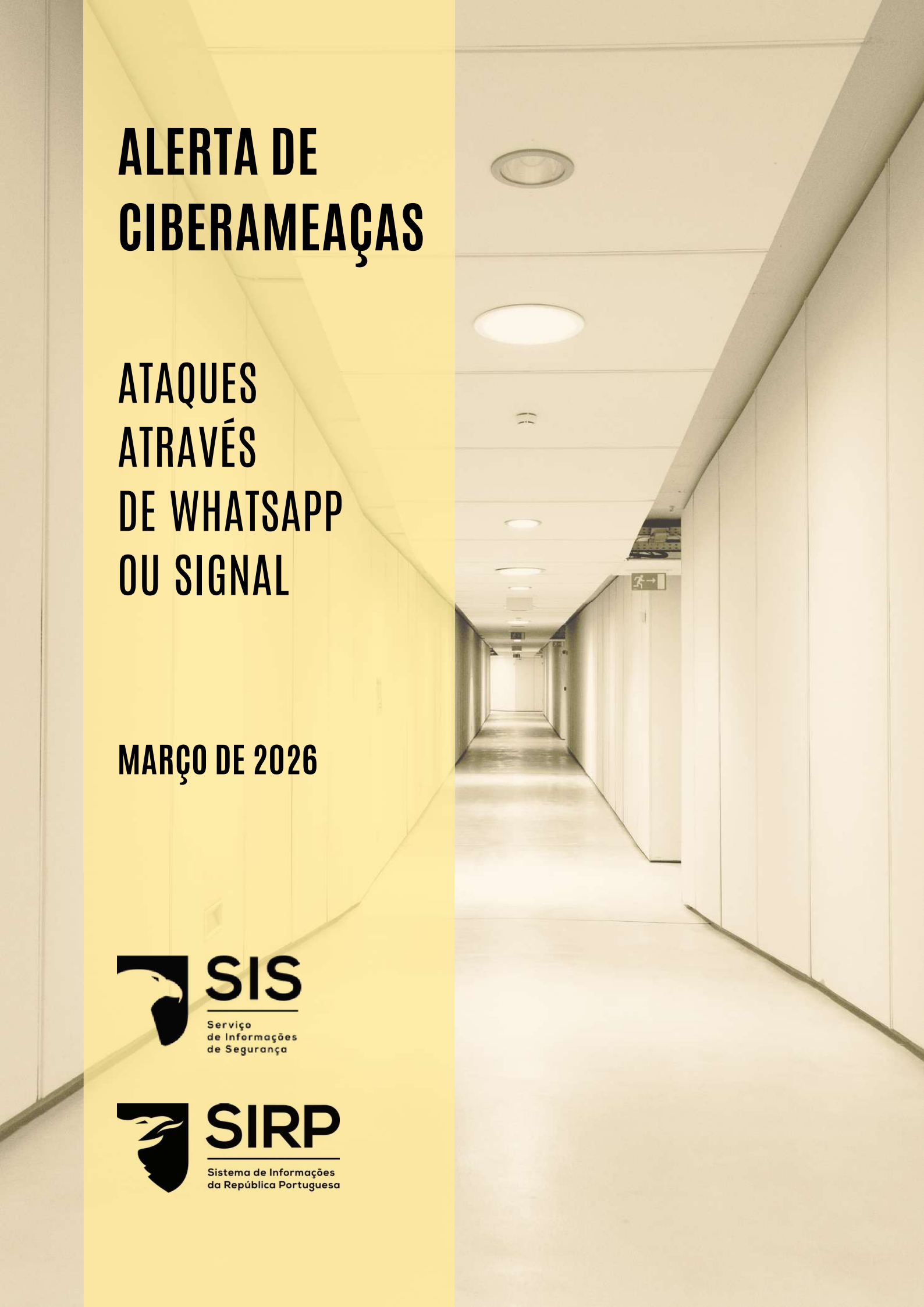
# ALERTA DE CIBERAMEAÇAS

## ATAQUES ATRAVÉS DE WHATSAPP OU SIGNAL

MARÇO DE 2026



SIS
Serviço de Informações de Segurança

SIRP
Sistema de Informações da República Portuguesa

# ALERTA DE CIBERAMEAÇAS:

Agentes de ciberameaças ao serviço de um Estado estrangeiro estão a desenvolver operações de ciberespionagem de escala internacional, orientadas para o comprometimento de contas individuais de Whatsapp ou Signal, com vista à exfiltração de informação privilegiada.

# ALVOS:

Os agentes de ameaça **não comprometem as aplicações Whatsapp e Signal ou a sua encriptação, nem exploram vulnerabilidades técnicas nas mesmas ou nos equipamentos de telecomunicações.** O seu objetivo é levar os utilizadores a executarem ações que resultem na quebra da segurança das suas contas.

Os alvos destas operações são **decisores executivos dos setores governamental, diplomático, militar e membros da sociedade civil**, com acesso a informação privilegiada de origem nacional e aliada.

SIS

SIRP

# METODOLOGIA

Os agentes de ciberameaça responsáveis por estas operações recorrem a diferentes técnicas, combinando operações de *phishing* com abordagens de engenharia social.

## Falso suporte técnico

O atacante contacta os seus alvos, apresentando-se como parte do suporte técnico do Whatsapp ou do Signal, e alerta para a existência de um falso risco de segurança que obriga à partilha das credenciais e dos códigos de acesso às contas.

## *Phishing*

O atacante partilha com as vítimas *links* que, caso sejam ativados, podem levar ao comprometimento das contas e das comunicações associadas

## *Quishing*

O atacante partilha com as vítimas códigos QR que, caso sejam lidos, resultam no comprometimento das contas e das comunicações associadas.

## Cooptação de identidade

O atacante assume a identidade de contactos de confiança (como colegas, associados ou homólogos) e inicia um diálogo com as vítimas sobre um assunto de interesse comum, com o objetivo de extrair informação privilegiada.

SIS

SIRP

# INTELIGÊNCIA ARTIFICIAL

Para credibilizar os ciberataques baseados em *phishing* e em engenharia social, os atacantes recorrem, cada vez mais, a ferramentas de Inteligência Artificial (IA) que lhes permitem, de uma forma muito rápida e plausível:

**Assumir coberturas institucionais**

O atacante pode fazer-se passar por *chatbots* ou funcionários das unidades de suporte técnico das aplicações ou de organizações internacionais para levar as vítimas a partilharem códigos de acesso às suas contas.

**Assumir identidades alheias**

Depois de recolher registos de imagem e de voz de pessoas da confiança dos alvos, o atacante pode replicá-las para fazer-se passar por esses mesmos indivíduos. As ferramentas de IA permitem manter conversações em áudio ou até por videochamadas.

Obter fluência linguística

Através de ferramentas de IA, o atacante consegue manter conversas de forma natural e fluente na língua nativa dos alvos ou das identidades assumidas. Esses diálogos dinâmicos podem ocorrer por mensagem, chamada telefónica ou videochamada.

# CONSEQUÊNCIAS

Estas operações de ciberespionagem visando utilizadores de Whatsapp e de Signal têm como consequências o comprometimento da segurança das respetivas contas e a exfiltração de informação privilegiada, posteriormente usada a favor do Estado estrangeiro.

Estas ações materializam-se, em particular, nos seguintes domínios:

**Adição de dispositivos não-autorizados**

O atacante adiciona dispositivos às contas no Whatsapp e no Signal e passa a poder, de forma invisível, monitorizar as comunicações das vítimas.

**Acesso a comunicações do alvo**

O agente de ameaça obtém acesso direto às comunicações do alvo por via do Whatsapp e do Signal.

***Take over* de contas**

Ao assumir a administração das contas comprometidas, o ciberatacante pode, mesmo, executar um *lock out* ao utilizador legítimo.

**Acesso a conversas em grupo**

O ator hostil passa a integrar os grupos de Whatsapp e de Signal em que o alvo participa.

**Elicitação de informação**

Através de operações de engenharia social, o atacante leva o alvo a partilhar informação de elevada sensibilidade.

**Novas ações de *phishing***

O agente de ameaça pode executar ações de *phishing* sob a cobertura da identidade digital do alvo inicial.

# PROTEÇÃO

Para a mitigação desta ameaça recomendam-se as seguintes medidas de implementação simples e imediata:

**Verificar**, por meios alternativos, **a veracidade de todas as novas interações e de novos contactos** no Whatsapp e no Signal .

**Nunca partilhar credenciais e códigos** de verificação das contas.

**Limitar a leitura de códigos QR** no Whatsapp ou no Signal a situações justificadas e iniciadas pelo próprio.

**Não permitir a adição não autorizada a grupos** de conversação no Whatsapp ou Signal.

**Maximizar as definições de segurança e de privacidade** das contas nas aplicações Whatsapp ou Signal.

**Reportar todas as situações suspeitas ou hostis** à sua unidade de cibersegurança institucional e às entidades nacionais competentes.

# CONTACTE-NOS

**Este ALERTA não significa que tenha ocorrido qualquer comprometimento do Whatsapp ou do Signal, ou a exploração de vulnerabilidades técnicas nestas aplicações.**

Ao invés, **reporta-se a operações de ciberespionagem que visam comprometer utilizadores mais expostos e vulneráveis**, que são os alvos prioritários dos diferentes agentes de ciberameaças.

Caso queira reportar uma situação de potencial ciberameaça, **contacte-nos através dos meios disponíveis em https://sis.sirp.pt.**

SIS
Serviço de Informações de Segurança

SIRP
Sistema de Informações da República Portuguesa