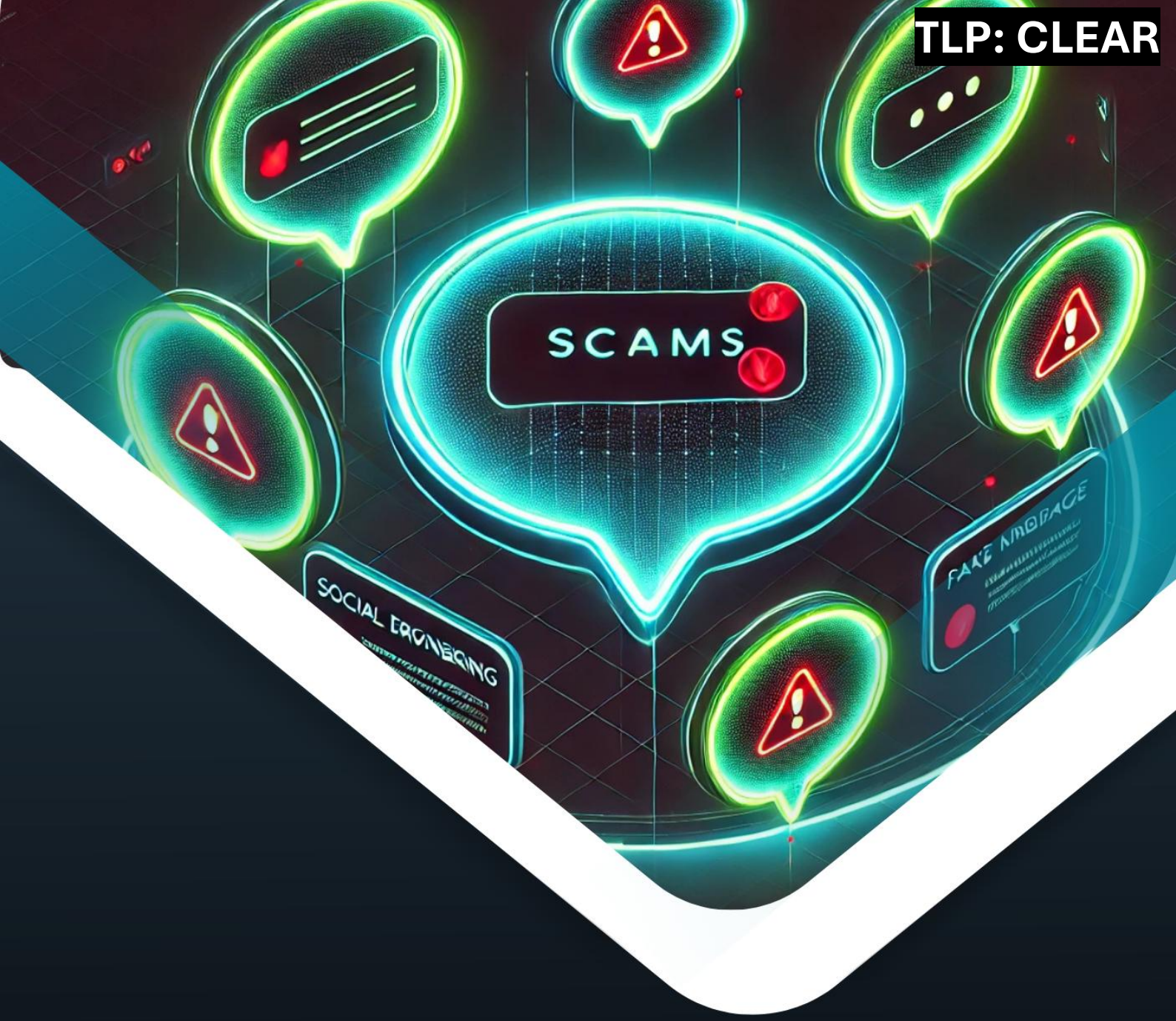
TLP: CLEAR



BOLETIM DE SEGURANÇA

Golpe de compartilhamento de tela no WhatsApp (Screen-Sharing Scam)

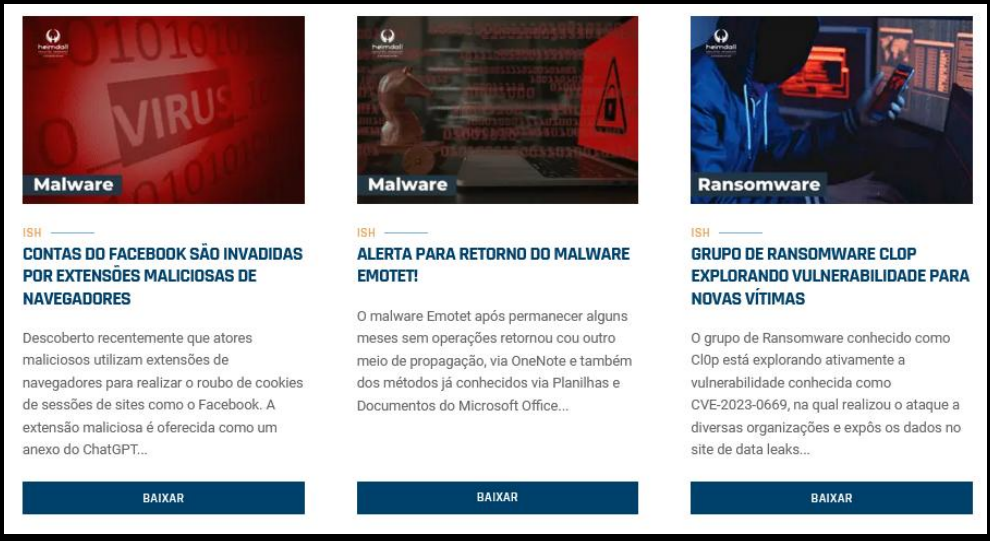
heimdall
security research

Acesse a nossa nova comunidade através do WhatsApp!

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



SUMÁRIO

1 SUMÁRIO EXECUTIVO

Está sendo observado um novo golpe em rápida expansão que explora o recurso de **compartilhamento de tela em chamadas de vídeo do WhatsApp** para roubar dados sensíveis, assumir contas e realizar fraudes financeiras. Diferente de ataques clássicos baseados em malware, este golpe é **predominantemente de engenharia social**: o criminoso manipula o usuário para que ele mesmo exponha senhas, códigos de verificação, dados bancários e outras informações críticas, **sem que exista, inicialmente, um arquivo malicioso ou hash para detecção**.

Casos já foram reportados em diversos países, incluindo um incidente com perda de cerca de **US$ 700.000** em uma única fraude.

1.1 OBJETIVO DO ATACANTE

O objetivo principal é:

- **Obter visibilidade total da tela do dispositivo da vítima** durante uma chamada de vídeo;
- **Capturar códigos de autenticação (OTP/2FA), senhas e dados bancários** exibidos na tela;
- **Assumir contas** (WhatsApp, e-mail, redes sociais, bancos, fintechs);
- **Realizar transações financeiras** e, em seguida, usar a própria identidade da vítima para aplicar golpes em familiares e contatos.

2 CADEIA DE ATAQUE - PASSO A PASSO

A seguir apresentamos, de forma estruturada, a **cadeia de ataque típica** associada a esta ameaça. O objetivo é oferecer uma visão completa do fluxo operacional utilizado pelos golpistas, desde o contato inicial até a execução da fraude.

2.1 PREPARAÇÃO DO GOLPE (FASE PRÉ-ATAQUE)

1. **Escolha das vítimas:**

- Usuários comuns de WhatsApp, muitas vezes em regiões onde o app é predominante para comunicação pessoal e com bancos.
- Alvos podem ser aleatórios (listagens de números) ou escolhidos (ex.: clientes de um banco específico).

2. **Infraestrutura de origem:**

- Uso de **números de telefone com DDD local** ou aparentemente legítimos para aumentar a confiança.
- Possível uso de linhas VoIP descartáveis ou SIMs pré-pagos.

3. **Roteiros de engenharia social:**

- Roteiros prontos para se passar por:
    - Funcionário de banco / operadora de cartão;
    - Suporte do WhatsApp / Meta;
    - Representante de serviço conhecido;
    - Parente ou amigo em situação de emergência.

2.2 CONTATO INICIAL - A CHAMADA NO WHATSAPP

- O ataque normalmente se inicia por uma chamada de vídeo ou, em alguns casos, apenas de áudio realizada via WhatsApp a partir de um número desconhecido. Na abordagem inicial, o golpista se apresenta como um representante legítimo, podendo se passar por “central de segurança do banco”, “equipe de suporte WhatsApp/Meta”, “equipe antifraude”, ou até mesmo fingir ser um parente ou amigo que teria “trocado de número” para reforçar a credibilidade. Para reduzir o risco de identificação e manter a vítima focada apenas na narrativa, os criminosos frequentemente utilizam estratégias de dissimulação visual, como manter a câmera apagada, o ambiente escuro ou a imagem propositalmente desfocada, dificultando qualquer reconhecimento e reforçando o caráter enganoso da interação.

2.3 Criação do problema (gatilho emocional)

Em seguida, o golpista cria um **cenário de urgência** para forçar decisões impulsivas:

- Alega:
    - Cobrança não reconhecida no cartão;
    - Acesso suspeito à conta em outro dispositivo;
    - Necessidade de "verificação urgente" para evitar bloqueio da conta;
    - Liberação de um suposto prêmio ou benefício que "vai expirar".

Objetivo: gerar medo, pressa e sensação de risco imediato, diminuindo o senso crítico da vítima.

2.4 Pedido de compartilhamento de tela/ acesso remoto

Com a confiança mínima estabelecida e a urgência criada, o invasor passa à etapa crítica:

1. **Solicita o compartilhamento de tela pelo próprio WhatsApp**, alegando que precisa "ver o que está acontecendo no aparelho" ou "guiar o procedimento de segurança".
2. Em alguns casos, o criminoso **orienta a instalação de aplicativos de acesso remoto legítimos**, como *AnyDesk*, *TeamViewer* ou *similares*, dizendo que são ferramentas oficiais de suporte.
3. Uma vez ativo o compartilhamento de tela (ou o app remoto):
    - Tudo o que aparece na tela da vítima passa a ser visível em tempo real para o atacante.

2.5 Coleta de dados sensíveis e comprometimento de contas

Com a tela exposta, o golpista passa a orientar ações específicas, sempre sob a narrativa de "resolver o problema":

1. **Captura de códigos de verificação e OTPs**

- O criminoso induz a vítima a:
    - Abrir SMS de autenticação;
    - Exibir códigos de WhatsApp, e-mail ou banco;
    - Navegar até apps financeiros.
        - Esses códigos permitem **tomar controle de contas** (WhatsApp, e-mail, bancos, redes sociais) em tempo real.

2. **Roubo de credenciais e dados bancários**

- Durante o processo, são observados:
    - Usuário/senha de internet banking ou apps de pagamento;
    - Números de cartão, CVV, validade, limites;
    - Respostas a perguntas de segurança.

3. **Possível instalação de malware adicional** (em alguns cenários)

- A mesma engenharia social pode ser usada para fazer a vítima:
    - Baixar aplicativos maliciosos (ex.: keyloggers disfarçados);
    - Ativar permissões excessivas no caso do Android.

2.6 Execução da fraude financeira e movimentações

- Com as informações capturadas durante o golpe, o criminoso inicia a execução da fraude financeira. A primeira etapa costuma ser a **tomada de contas**, registrando o WhatsApp da vítima em outro dispositivo a partir do código de verificação que foi exposto na tela e, sempre que possível, procedendo à troca de senhas de e-mail, redes sociais e serviços bancários, consolidando o controle sobre os principais canais da vítima. Em seguida, parte-se para as **transações financeiras**, aproveitando o acesso obtido para realizar transferências bancárias, pagamentos de boletos, compras on-line e até operações instantâneas, como Pix, dependendo do país já tendo sido relatados casos em que as perdas alcançaram centenas de milhares de dólares para uma única vítima. Paralelamente, o golpista utiliza a identidade comprometida para **novos golpes**, explorando o fato de ter o WhatsApp da vítima sob total controle para pedir dinheiro a familiares e amigos, enviar links maliciosos e ampliar a cadeia de vítimas manipulando a confiança do círculo social da pessoa afetada.

2.7 Encerramento e encobrimento

Após a fraude:

- O atacante:
    - Desloga o usuário das sessões legítimas;
    - Apaga históricos de conversas;
    - Pode trocar foto, nome e configurações de privacidade para dificultar o reconhecimento.

A vítima, normalmente, só percebe o golpe **quando já houve débito em conta ou quando contatos começam a estranhar pedidos de dinheiro**.

3 INDICADORES DE ATAQUE (COMPORTAMENTAIS)

Como não há, na fase inicial, arquivo malicioso ou URL obviamente maliciosa, é importante observar **indicadores comportamentais**:

Chamada de vídeo/voz não solicitada de número desconhecido se passando por:

- Banco, suporte WhatsApp/Meta, operadora ou órgão oficial.

Discurso com forte senso de urgência, falando em:

- Bloqueio imediato de conta;
- Cobranças suspeitas;
- Necessidade de confirmação “agora”.

Pedido explícito de:

- Compartilhamento de tela do celular/computador;
- Instalação de app de acesso remoto;
- Exibição de SMS, e-mails ou notificações de código de verificação.

Orientações fora do padrão de bancos/empresas, como:

- Pedir para informar senhas, códigos de token, PIN de cartão;
- Solicitar que a pessoa realize transferências “para validar conta”.

4 RECOMENDAÇÕES

São elencadas abaixo pela ISH, medidas que poderão ser adotadas visando a mitigação da infecção da referida *ameaça*, como por exemplo:

4.1 RECOMENDAÇÕES PARA USUÁRIOS FINAIS

Nunca compartilhar a tela com desconhecidos

- Não aceite pedidos de compartilhamento de tela em chamadas de WhatsApp com números que você não conhece ou não tenha verificado por outro canal.

Desconfiar de qualquer contato que crie urgência

- Bancos e empresas sérias **não pressionam pelo imediatismo** em ligações ou WhatsApp para que você compartilhe tela ou códigos.

Jamais informar senhas, PINs ou códigos de verificação

- Nenhum atendente legítimo deve pedir seu código de WhatsApp, código de SMS, token, CVV ou senha de cartão.

Confirmar o contato por canal oficial

- Se o suposto banco/empresa ligar:
  - Desligue a chamada;
  - Ligue você mesmo para o número oficial do banco / acesse o app oficial;
  - Confirme se há realmente qualquer problema.

Ativar a verificação em duas etapas no WhatsApp

- Habilitar a proteção com PIN adicional nas configurações de conta, para dificultar a tomada de controle mesmo que o invasor veja um código de SMS.

Manter sistema e apps atualizados

- Atualizar sistema operacional e aplicativos regularmente, incluindo apps de segurança.

4.2 RECOMENDAÇÕES PARA A ORGANIZAÇÃO

Campanhas de conscientização

- Divulgar este alerta internamente para todos os colaboradores;
- Incluir exemplos reais (sem dados sensíveis) de como o roteiro da fraude se apresenta.

Diretrizes oficiais de suporte

- Reforçar que **ninguém da organização** está autorizado a:
    - Pedir compartilhamento de tela via WhatsApp a clientes/terceiros;
    - Solicitar instalação de AnyDesk, TeamViewer ou similares para "suporte".

Políticas de uso de WhatsApp corporativo

- Definir claramente:
    - Em que situações será usado;
    - Como o time deve se identificar;
    - Quais informações nunca devem ser solicitadas por esse canal.

Monitoramento e resposta

- Criar playbook de resposta para casos em que:
    - Colaborador ou cliente informe ter compartilhado tela com suposto suporte;
    - Haja indício de comprometimento de conta.

Integração com o SOC / time de segurança

- Acompanhar notícias e atualizações sobre este golpe e outras variantes de engenharia social;
- Adequar campanhas de simulação de phishing/engenharia social incluindo **cenários de vídeo-chamada e pedido de compartilhamento de tela**.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **ESET**

6 AUTORES

- **Heimdall *by* ISH Tecnologia**

heimdall
security research
A DIVISION OF ISH