Departamento de Segurança da Informação e Comunicações – **DSIC** dsic.planalto.gov.br/
Centro de Tratamento de Incidentes de Redes do Governo – **CTIR Gov** www.ctir.gov.br/

Recomendação nº 01/2018

Golpe de Clonagem de Contas do Aplicativo WhatsApp

Público Alvo: Integrantes da Administração Pública e Entidades Vinculadas

1. Descrição

Data de Publicação: 13/04/2018
Data de Atualização: 13/04/2018

Com mais de um bilhão de usuários ativos espalhados pelo mundo, no Brasil o aplicativo WhatsApp Messenger também torna a troca de mensagens instantâneas um dos principais usos dos aparelhos móveis, como celulares ou smartphones. Em função dessa popularidade, o WhatsApp já é uma ferramenta considerada estratégica por diversas empresas, inclusive com bastante difusão entre órgãos e servidores públicos por todo o País e representações no exterior.

O aplicativo faz a identificação dos seus usuários entre os contatos registrados no telefone, coletando seus dados, com a finalidade de fazer a equiparação eficientemente, o que é usado por alguns formatos de golpes. Entre eles, um tem sido observado de forma constante entre usuários, membros da administração pública.

Esse golpe consiste da clonagem de contas de WhatsApp, em que, como procedimento, o golpista indisponibiliza o telefone celular da vítima, assume a conta do aplicativo e realiza o envio de mensagens, solicitando transferências bancárias a amigos e família.

2. Impacto

A clonagem de números e o registro de golpes com o uso de mensagens via WhatsApp têm se tornado cada vez mais comuns e, desde 2017, servidores públicos têm sido vítimas, com maior frequência. Nesse golpe, os criminosos clonam a número do aparelho celular para, em seguida, sequestrar a conta do WhatsApp, vindo a se passar pelos reais proprietários, pedindo auxílios bancários como depósitos e pagamento de boletos. Como justificativa, informam que estão com dificuldade de acessar o banco e por isso precisam do favor com urgência, ou que estão em sérias dificuldades financeiras.

Ao invadir uma conta de WhatsApp, os falsários podem acessar o histórico de conversas, os grupos e contatos, o que pode incluir dados pessoais e detalhes que só as vítimas sabem. Isso torna os pedidos de transferência de dinheiro mais convincentes. O golpista pode identificar quem são os parentes, quem são os amigos e tem informações que podem fazer o golpe mais efetivo.

Quando o chip é clonado, o telefone celular original do usuário daquele chip passa a não efetuar ou receber ligações, bem como perde seu serviço de dados, deixando-o sem Internet móvel, sendo assim, o seu proprietário pode considerar existir uma pane temporária no aparelho ou na operadora, levando-o a demorar a tomar providências. Durante esse tempo os golpistas realizam a instalação do aplicativo WhatsApp em outro aparelho e podem alterar configurações originais, com o chip clonado, podendo fazer uso de qualquer rede *Wi-Fi.* Logo a vítima perde o acesso à sua conta de WhatsApp, mesmo recuperando seu chip da operadora.

3. Dispositivos Afetados

Qualquer dispositivo móvel com acesso à Internet, que tenha sistema operacional Android, BlackBerry OS, iOS, Symbian, Windows Phone e Nokia.

4. Recomendações

4.1 Prevenção

- Mantenha o aplicativo atualizado. Correções de segurança são disponibilizadas periodicamente sem que os usuários percebam diferença no seu funcionamento. É fundamental instalar as atualizações para minimizar os riscos à segurança das mensagens.
- Proteja a conta do WhatsApp por meio da "Verificação de duas etapas". Conforme citação no site do WhatsApp, a verificação em duas etapas é um recurso opcional para adicionar mais segurança à conta do aplicativo. Ao se ativar a verificação em duas etapas, qualquer tentativa de verificação do número de telefone no WhatsApp terá que ser acompanhada de um PIN de seis dígitos criado.
    - Para ativar a verificação em duas etapas, abra o WhatsApp e vá em: **configurações > conta > Verificação em duas etapas > Ativar**. Ao ativar este recurso, será oferecida a opção de inserir um endereço de e-mail. Este endereço de e-mail será utilizado para que o WhatsApp possa enviar um link para desativar a verificação em duas etapas no caso de esquecimento do PIN, servindo como uma proteção à sua conta.
- Proteja o *smartphone* com senha. Quando o *smartphone* é perdido ou roubado, o vazamento das informações que o mesmo constar pode gerar grande aborrecimento e prejuízo. Por isso, é importante habilitar o bloqueio da tela e protegê-lo por meio de senha pessoal. Evite manter fotos, vídeos e mensagens de voz armazenadas no aparelho, pois elas podem ser acessadas por pessoas não autorizadas.

- Evite armazenar arquivos pessoais no cartão de memória. Os dispositivos móveis, nem sempre, oferecem espaço interno suficiente para a armazenagem de arquivos. Usuários acabam por instalar cartões de memória, mas deve-se evitar salvar arquivos pessoais nesse dispositivo de armazenamento devido a facilidade de leitura em outros aparelhos ou computadores pessoais. Mesmo quando os arquivos pessoais são apagados, eles podem ser facilmente recuperados.
- Utilize aplicativos que apagam definitivamente os arquivos excluídos. Existem aplicativos que permitem a recuperação de arquivos que foram apagados acidentalmente, sendo que esse mesmo tipo de recurso pode ser utilizado para reaver arquivos pessoais que estavam armazenados no cartão de memória. Para dificultar essa ação, instale um aplicativo chamado "*Secure delete*", disponível gratuitamente na *Google Play*.
- Apague todos os arquivos pessoais e senhas salvas quando for levar o aparelho para manutenção. Os dispositivos móveis estão sujeitos a manutenções e, dependendo do tipo de manutenção que será realizada, poderá ser necessário entregá-lo desbloqueado para testes. Nesse caso, é prudente apagar todos os arquivos pessoais, remover o *Sim Card* (chip da operadora), e senhas salvas em aplicativos.
- Não forneça dados pessoais para confirmação em chamadas telefônicas de números desconhecidos. É usual se receber chamadas telefônicas em que o operador solicita dados para confirmação. Pela dificuldade de identificação da origem, deve-se evitar o fornecimento de informações pessoais! Quem possui o acesso ao sistema é quem deve se encarregar de verificar a veracidade das informações contidas no cadastro. Importante salientar que tal procedimento deve ser tomado ao se receber a ligação, pois no caso de o cliente entrar em contato com os serviços de atendimento, certificando a correção do número, é necessário o respeito às regras de atendimento.
- Desconfie dos pedidos de ajuda por meio de aplicativos ou redes sociais. Desvios de segurança, algumas vezes por parte do próprio usuário, são comuns no uso de aplicativos para troca de mensagens e redes sociais. O mesmo pode ser aplicado ao uso de *smartphone,* se o mesmo estiver desprotegido e com as senhas salvas nos aplicativos. Como prevenção, é recomendável, ao se receber um pedido de ajuda, retornar a mensagem através de uma ligação telefônica e se certificar que o autor da mensagem é realmente a pessoa que está pedindo ajuda.

4.2 Mitigação em caso de suspeita de ter o WhatsApp clonado

O WhatsApp clonado no celular de outra pessoa pode mostrar todas as mensagens em tempo real, ainda que não tenha o mesmo chip da operadora. Em caso de suspeita de ter o WhatsApp clonado, siga as sugestões a seguir:

- Desconectar do WhatsApp Web
  - Passo 1. Existem aplicativos de terceiros que permitem clonar o WhatsApp no celular ou computador de outras pessoas, usando o acesso do WhatsApp Web no celular. O primeiro passo para se livrar de alguém vendo suas mensagens é desconectar dessas contas. Para isso, toque no menu indicado por "três pontos" no topo direito e selecione "WhatsApp Web".
  - Passo 2. Em "Sessões Ativas", estarão listados os navegadores nos quais se está conectado. Não reconhecendo as sessões, pressione "Sair de todos os computadores" e confirme em "Sim". Será necessário reconectar, em caso de uso em máquinas de confiança. Na dúvida, realizar sempre *logout* no WhatsApp Web, mesmo no próprio computador.
- Ativar o código de verificação em duas etapas
  - Passo 1. O código de verificação em duas etapas permite adicionar uma senha "extra" para ativar o WhatsApp, que é solicitada no aplicativo ao reinstalá-lo ou esporadicamente, para garantir a privacidade. Para ativar, pressione o menu do topo do WhatsApp e selecione "Configurações".
  - Passo 2. Em seguida, toque em "Conta" e selecione "Verificação em duas etapas".
  - Passo 3. Pressione no botão de "Ativar". Em seguida, será necessário adicionar um código pessoal (PIN) com seis dígitos (criado por você) e depois digitá-lo novamente para confirmar. Toque em "Avançar" em cada etapa.
  - Passo 4. Se preferir, adicione também um e-mail pessoal para recuperação do acesso e, ao final, confirme em "Concluído".
- Apagar o histórico de uma conversa
  - Passo 1. No caso de se considerar que a conta do WhatsApp está em risco, uma medida emergencial é apagar conversas que tenham dados pessoais, principalmente financeiros. Para isso, abra a conversa e toque no ícone de menu (três pontos) no topo da tela. Em seguida, pressione "Mais". Depois selecione "Limpar conversa".
  - Passo 2. Confirme a ação em "Limpar", inclusive as mensagens marcadas (se necessário). Note que o *chat* aparecerá vazio. Assim a pessoa que realizou a clonagem não vai mais ter acesso àquelas informações.
- Ver se alguém leu sua mensagem
  - Passo 1. Quando uma nova mensagem chega, ela é indicada por um marcador verde, tanto em conversas individuais, quanto em grupos. Note que esse marcador mostra, inclusive, quantas mensagens novas há na conversa. Dessa forma, você sabe que ninguém abriu o recado. No entanto, também existe o marcador de "mensagem não lida", que pode ser adicionado depois de ler a conversa. Ele, porém, é diferente: não tem número, apenas um ponto verde. Fique atento a essa mudança no seu mensageiro para pegar curiosos ou invasores.
- Reinstalar o WhatsApp
  - Passo 1. Uma outra ação para resolver o WhatsApp clonado é reinstalar o aplicativo. Com isso, o mensageiro vai pedir novamente o código de verificação e enviar o SMS para verificar o aparelho. Pode ser uma forma de anular a ação de terceiros em outros aparelhos. Para isso, acesse o menu de "Configurações" e toque em "Gerenciador de aplicações".
  - Passo 2. Encontre o WhatsApp na lista e depois toque em "Desinstalar". Uma sugestão é fazer o backup das mensagens do WhatsApp antes desse procedimento, para não perder nada na reinstalação. Depois, basta baixar novamente o aplicativo e refazer a instalação.

4.3 Mitigação em caso de aparelho celular perdido ou roubado

O WhatsApp oferece um serviço de segurança para desativar a conta do mensageiro à distância, ideal para casos em que o celular foi perdido ou roubado e não se quer que outros utilizem sua conta. Assim, o usuário mantém seus dados e conversas no aplicativo protegidos e o procedimento pode ser feito de qualquer outro dispositivo móvel ou PC. É necessário enviar um e-mail padrão para encerrar a conta no WhatsApp, para proteger sua privacidade, e bloquear o *Sim Card* (chip da operadora).

- Desativar a conta diretamente com o WhatsApp. Para maior segurança, o usuário pode desativar a conta do WhatsApp usando um outro celular ou computador, principalmente se ainda não tiver um celular ativo com mesmo número (por meio de portabilidade). Neste procedimento, basta enviar uma mensagem de *e-mail* padrão para o serviço mensageiro, usando qualquer outro aparelho com conexão à Internet e serviço de *e-mail* (Gmail, Outlook, Yahoo Mail e outros).
    - Passo 1. Abra o aplicativo de *e-mail* no seu celular ou PC. Inicie a criação de uma nova mensagem de *e-mail* que deve ser enviado para o destinatário *support@whatsapp.com*. O assunto deve ser "Perdido/Roubado: Por favor, desative minha conta" (sem as aspas).
    - Passo 2. No corpo do e-mail, escreva também "Perdido/Roubado: Por favor, desative minha conta". Em seguida digite o número do celular atrelado ao WhatsApp no formato internacional, com "(+) número do país + DDD + número do telefone". No caso do Distrito Federal, no Brasil, um exemplo seria: +55(61) 9XXXX-XXXX no qual "55" é o código do país, "61" o DDD local e depois o número do celular. Em seguida, envie o e-mail.
- Sobre a conta desativada. Depois de enviar o *e-mail*, a conta não é totalmente apagada pelo prazo de 30 dias. O usuário tem esse limite de tempo para reativar em outro aparelho celular. Desta forma, os contatos ainda podem enviar mensagens, que ficam pendentes por até 30 dias. Depois que reativar, o usuário receberá esses recados e poderá recuperar os grupos. Além disso, o nome de usuário ainda aparecerá na lista de contatos dos seus amigos.
- Bloquear o *Sim Card* (chip da operadora). Uma recomendação do WhatsApp que ajuda a desativar uma conta no aplicativo de forma mais prática é fazer o bloqueio do *Sim Card* (chip da operadora). Para isso, contate a operadora e solicite a operação. Esse procedimento deve ser feito assim que o celular for roubado ou perdido. Isso é importante porque o WhatsApp só pode estar ativo em um número de telefone e aparelho de cada vez. Assim, quando o usuário for cadastrar o aplicativo no novo celular, com mesmo número (após a portabilidade), o antigo será desconsiderado por não ter confirmação via SMS para verificar a conta. Vale lembrar que mesmo com o chip bloqueado ainda será possível usar o WhatsApp via Wi-Fi no celular roubado/perdido, caso o desligamento não seja feito via e-mail para o WhatsApp ou tenha transferência para um novo aparelho.

Importante frisar, conforme consta nas orientações da Agência Nacional de Telecomunicações (Anatel), que a vítima de celular clonado deve comunicar à operadora telefônica e pedir o bloqueio da linha, além de solicitar esclarecimentos sobre o que foi registrado no caso.

Por fim, a Anatel orienta sobre indícios que podem indicar que um celular foi clonado: dificuldades para completar chamadas originadas; quedas frequentes de ligação; dificuldade para acesso à caixa de mensagem; chamadas recebidas de números desconhecidos, nacional e internacional; e débitos de prestação de serviços muito acima da média.

5. Referências

- CRIME VIRTUAL - Entenda como funciona golpe no WhatsApp que vitimou deputados federais. Disponível em: <https://www.conjur.com.br/2018-fev-10/entenda-funciona-golpe-whatsapp-vitimou-deputados> Acesso em: 02 abr. 2018.
- G1 - Golpe clona contas de WhatsApp para pedir dinheiro a contatos de vítimas. Disponível em: <http://g1.globo.com/rs/rio-grande-do-sul/noticia/2017/02/golpistas-clonam-contas-de-whats-app-para-pedir-dinheiro-contatos.html> Acesso em: 02 abr. 2018.
- G1 - Depois de caso de Cida Borghetti, deputado Romanelli também tem celular clonado. Disponível em: < https://g1.globo.com/pr/parana/noticia/depois-de-caso-de-cida-borghetti-deputado-romanelli-tambem-tem-celular-clonado.ghtml> Acesso em: 02 abr. 2018.
- Segurança do WhatsApp. Disponível em: <https://www.whatsapp.com/security/> Acesso em: 04 abr. 2018.
- Dicas e Tutoriais TechTudo - Como desativar uma conta no WhatsApp caso celular seja perdido ou roubado. Disponível em: <http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2016/06/como-desativar-uma-conta-no-whatsapp-caso-celular-seja-perdido-ou-roubado.html> Acesso em: 04 abr. 2018.
- G1 - Tecnologia e Games - WhatsApp: confira as dicas para proteger a sua conta. Disponível em: <http://g1.globo.com/tecnologia/blog/tira-duvidas-de-tecnologia/post/whatsapp-confira-dicas-para-proteger-sua-conta.html> Acesso em: 04 abr. 2018.
- Dicas e Tutoriais TechTudo - WhatsApp clonado? Veja como se proteger para ninguém acessar sua conta. Disponível em: <http://www.techtudo.com.br/dicas-e-tutoriais/noticia/2017/03/whatsapp-clonado-veja-como-se-proteger-para-ninguem-acessar-sua-conta.html> Acesso em: 04 abr. 2018.
- Perguntas Frequentes do WhatsApp - Apagando sua conta. Disponível em: <https://faq.whatsapp.com/pt_br/android/21119703/?category=5245246> Acesso em: 04 abr. 2018.
- Perguntas Frequentes do WhatsApp - Fique seguro no WhatsApp. Disponível em: <https://faq.whatsapp.com/pt_br/android/21197244/?category=5245250> Acesso em: 04 abr. 2018.
- Perguntas Frequentes do WhatsApp - Telefones perdidos ou roubados. Disponível em: <https://faq.whatsapp.com/pt_br/iphone/24460358/> Acesso em: 05 abr. 2018.
- Perguntas Frequentes do WhatsApp - Verificação em duas etapas. Disponível em: <https://faq.whatsapp.com/pt_br/android/26000021/?category=5245245> Acesso em: 05 abr. 2018.
- ANATEL - AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. Disponível em: < http://www.anatel.gov.br/institucional/> Acesso em: 05 abr. 2018.

Equipe do CTIR Gov – *ctir@ctir.gov.br*