Reportagem Especial

AMEAÇAS VIRTUAIS

Novo vírus pelo WhatsApp se espalha, rouba dados e contas

Chamado Sorvepotel, ele ataca computadores via WhatsApp Web, usando links ou anexos falsos para obter senhas e informações sigilosas

Eliane Proscholdt

O WhatsApp Web virou porta de entrada para ataque hacker em todo o País. A técnica utilizada pelos golpistas consiste em uma invasão silenciosa, que compromete o acesso do usuário sem que ele perceba. Assim, senhas e até o controle da conta podem ser roubados pelo novo vírus em poucos segundos.

Batizado de Sorvepotel, o golpe se baseia em softwares maliciosos enviados por meio de mensagens com anexos ou links — normalmente disfarçados como recibos, orçamentos ou comprovantes — com o objetivo de enganar internautas desavisados.

"Esse novo vírus está se propagando no WhatsApp, mas só consegue ser efetivo no Windows, ou seja, no WhatsApp Web do computador, não no celular. Para isso, a pessoa precisa clicar no link. A mensagem é enviada com um anexo — que pode estar no formato .zip, um arquivo compactado — ou no formato .pdf", explica Eduardo Pinheiro, especialista em proteção de dados.

Segundo ele, geralmente o nome desse arquivo é "comprovante". "Esse é o nome para instigar a pessoa a clicar. Quando a pessoa clica no WhatsApp Web, ela vai estar comprometendo o seu dispositivo, porque esse vírus abre a porta do computador para o invasor; aí ele consegue controlar todo o dispositivo, tendo acesso principalmente a dados bancários e também às senhas", contou Eduardo Pinheiro.

O Tribunal de Justiça do Espírito Santo (TJES) vem sendo alvo desse tipo de ataque e, por isso, adotou medidas de proteção.

Como forma preventiva, o Comitê Gestor de Segurança da Informação (CGSI) deliberou que o acesso ao WhatsApp Web fosse temporariamente bloqueado nas redes institucionais, visando resguardar os dados e a segurança digital dos usuários.

"Como medida corretiva aos eventos já identificados, a ação tomada pela STIC (Secretaria de Tecnologia da Informação e Comunicação) é a formatação dos computadores infectados, o que leva a longas indisponibilidades das estações de trabalho. O acesso será restabelecido assim que houver garantias técnicas adequadas".

A reportagem apurou que o bloqueio do WhatsApp Web no Tribunal de Justiça começou na última sexta-feira e, até ontem, ainda não havia sido restabelecido.

O titular da Delegacia Especializada de Repressão aos Crimes Cibernéticos (DRCC), delegado Brenno Andrade, ressalta que esse golpe tem as mesmas características que a polícia sempre alerta, ou seja, é aplicado no sentido de obter dados indevidamente das pessoas.

Portanto, a orientação é não clicar em arquivos desconhecidos, mesmo que tenham sido enviados por contatos conhecidos, já que esses perfis podem ter sido comprometidos e o vírus pode estar se espalhando a partir deles.

FÁBIO NUNES — 22/05/2023

BRENNO ANDRADE disse que o golpe segue o padrão clássico de ataques que visam obter dados de forma ilegal

SAIBA MAIS

Como é

> **O GOLPE COMEÇA QUANDO** o usuário recebe um arquivo ZIP (aparentemente inofensivo, como um comprovante), que contém um atalho malicioso.

> **AO SER ABERTO**, o vírus se instala no computador da vítima e passa a enviar automaticamente o mesmo arquivo para outros contatos e grupos do WhatsApp Web, se espalhando rapidamente.

> **O OBJETIVO DESSA AMEAÇA**, neste momento, é o roubo de informações bancárias, incluindo usuários, senhas e contra-senhas de acesso aos bancos brasileiros.

> **O MALWARE** pode permitir o acesso remoto ao computador da vítima, abrindo portas para ataques mais graves.

Medidas de prevenção

> **EVITE ABRIR ARQUIVOS** ZIP ou links suspeitos, manter o antivírus atualizado, ativar a verificação em duas etapas no WhatsApp e não use o WhatsApp Web em dispositivos públicos ou desprotegidos.

> **DESCONECTAR** o WhatsApp Web quando não estiver em uso.

O que fazer em caso de infecção

Se suspeitar que foi atingido pelo Sorvepotel, as recomendações são:

> **DESCONECTAR** imediatamente o dispositivo da internet para interromper a propagação;

> **FAZER UMA VARREDURA** completa com um antivírus confiável;

> **ALTERAR SENHAS** de acesso de contas que possam ter sido comprometidas;

> **AVISAR CONTATOS** para que não cliquem ou abram arquivos que venham automaticamente do dispositivo infectado;

> **REGISTRAR** um boletim de ocorrência, para formalizar o ataque.

DIVULGAÇÃO

ACESSO AO WHATSAPP WEB: cuidados para não abrir arquivos suspeitos e nem clicar em links desconhecidos

O OUTRO LADO

Ações tomadas

O WhatsApp informou, por meio de sua assessoria de imprensa, que ações estão sendo tomadas para prevenir os golpes, mas a proteção individual também é importante.

"Estamos sempre trabalhando para tornar o WhatsApp o lugar mais seguro para a comunicação privada, e é por isso que criamos camadas de proteção que oferecem mais contexto sobre com quem você está conversando ao receber uma mensagem de alguém que você não conhece — além de proteger suas conversas pessoais com a criptografia de ponta a ponta", afirma o comunicado enviado à imprensa.

Fraudes com Inteligência Artificial viram desafio

A Inteligência Artificial veio com a promessa de facilitar diversos setores da sociedade, mas, quando mal utilizada, pode se tornar uma arma poderosa nas mãos erradas.

Exemplo disso é a crescente proliferação de ferramentas de Inteligência Artificial, que têm facilitado a criação de vídeos e fotos falsos, tornando cada vez mais difícil distinguir o que é real de montagens altamente convincentes.

O titular da Delegacia Especializada de Repressão aos Crimes Cibernéticos (DRCC), delegado Brenno Andrade, lembra que, com a evolução dessa tecnologia, a própria IA, fica mais fácil para criminosos produzirem vídeos, simulações e montagens falsas.

CONTEÚDOS

Ao mesmo tempo, o delegado salienta que fica mais difícil para a polícia identificar esses conteúdos sem uma análise técnica mais detalhada.

"É um problema que as polícias, de uma forma geral, têm de se atentar para o presente e futuro, com a evolução da tecnologia cada vez mais rápida e crescente, a fim de poder identificar, de uma forma mais rápida e fidedigna, imagens geradas falsamente por meio da inteligência artificial", finalizou Brenno Andrade.

ANÁLISE

Carlos Augusto da Motta Leal, advogado, especialista em Direito Digital

"Cibercriminosos atualizam táticas"

"Nos últimos meses, golpes digitais sofisticados voltaram a mirar o WhatsApp Web, com destaque para o malware 'Sorvepotel'.

Disfarçado de comprovante em arquivo ZIP, o vírus instala-se no computador, capta dados bancários e rouba senhas de forma silenciosa. A partir de uma sessão ativa, replica-se automaticamente ao enviar o mesmo arquivo malicioso a contatos e grupos da vítima.

Órgãos públicos, como o TJES (Tribunal de Justiça), emitiram alertas e restringiram o uso do WhatsApp Web em suas redes.

O padrão se repete: cibercriminosos atualizam suas táticas, mas mantêm o objetivo: obter vantagem financeira por meio do roubo de dados.

Usuários devem redobrar a atenção: evitar abrir arquivos suspeitos, mesmo vindos de conhecidos, manter antivírus atualizados e desconfiar de mensagens com tom de urgência são medidas essenciais.

A conscientização ainda é a principal defesa contra esse tipo de golpe".