BOLETIM DE SEGURANÇA

Pesquisadores descobrem falhas de segurança em aplicações dos automóveis da Tesla

heimdall
security research
A DIVISION OF ISH

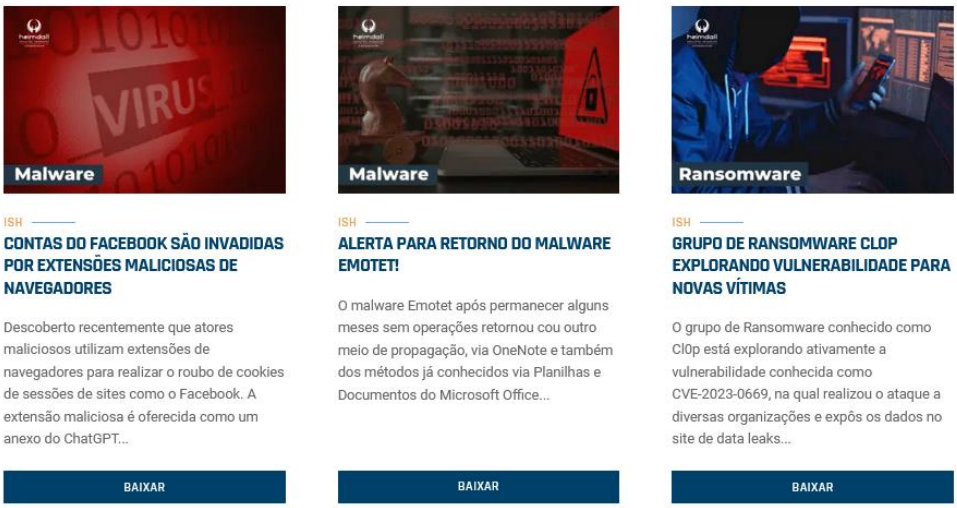
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

[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

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Os pesquisadores **Talal Haj Bakry** e **Tommy Mysk**, informaram a possibilidade de um ataque de phishing MITM utilizando o dispositivo **Flipper Zero** para comprometer as contas e desbloqueio dos carros da *Tesla*, recentemente utilizada nas versões mais recente (**4.30.60** e **11.1 2024.2.7**). Foi registrado como parte do ataque uma nova *'Phone key*' que poderia ser aprovada pelo Tesla e que ao vincular o carro a um telefone, há a necessidade de autenticação correta. Embora os testes realizando um ataque de phishing usando um Flipper Zero, ele poderia ser feito facilmente com outros dispositivos, como um computador, um Raspberry Pi ou até telefones Android.

2 O ATAQUE DE PHISHING

Nos testes realizados mostra como um invasor em uma estação de superalimentação Tesla poderia implantar uma rede WiFi chamada “Tesla Guest”, um SSID comumente encontrado em centros de serviço Tesla e que os proprietários de automóveis estão familiarizados com ele. O pesquisador Mysk utilizou-se do dispositivo Flipper Zero para transmitir a rede WiFi, porém o mesmo pode ser feito usando um Raspberry Pi ou outros dispositivos que vêm com recursos de **hotspot WiFi**.

Após a vítima se conectar à rede falsa, ela recebe uma página de login falsa do Tesla solicitando o login usando as credenciais da conta. Tudo o que a vítima digitar na página de **phishing**, o ator malicioso pode ver no dispositivo Flipper Zero em tempo real.

Após inserir as credenciais da conta Tesla, a página de phishing solicita a senha de uso da conta, para ajudar o invasor a contornar a proteção de autenticação de dois fatores. Ele precisa se mover antes que o OTP expire e fazer login no aplicativo Tesla usando as credenciais roubadas. Uma vez na conta, o invasor pode rastrear a localização do veículo em tempo real.

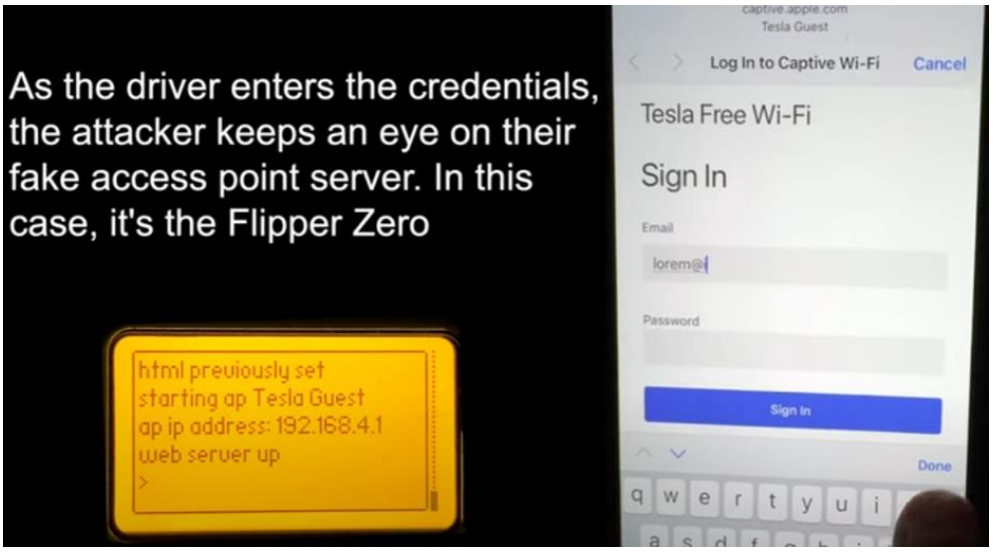


Figura 1 – Processo do phishing.

3 NOVA CHAVE ADICIONADA

O acesso à conta Tesla da vítima permite o invasor adicionar uma nova 'Phone key'. Para isso, devem estar próximos do carro, a poucos metros de distância. Essas Phone Keys utilizam o aplicativo móvel da Tesla em conjunto com o smartphone do proprietário do carro para permitir o travamento e destravamento automático do veículo, por meio de uma conexão Bluetooth segura. Os carros da Tesla também usam Card Keys, que nada mais são que cartões RFID finos que precisam ser colocados no leitor RFID do console central para dar partida no veículo. Embora mais seguros, a Tesla os trata como uma opção de backup se a chave do telefone estiver indisponível ou sem bateria. O pesquisador informou que adicionar uma nova Phone key por meio do aplicativo não exige que o carro esteja desbloqueado ou que o smartphone esteja dentro do veículo, criando uma lacuna de segurança.

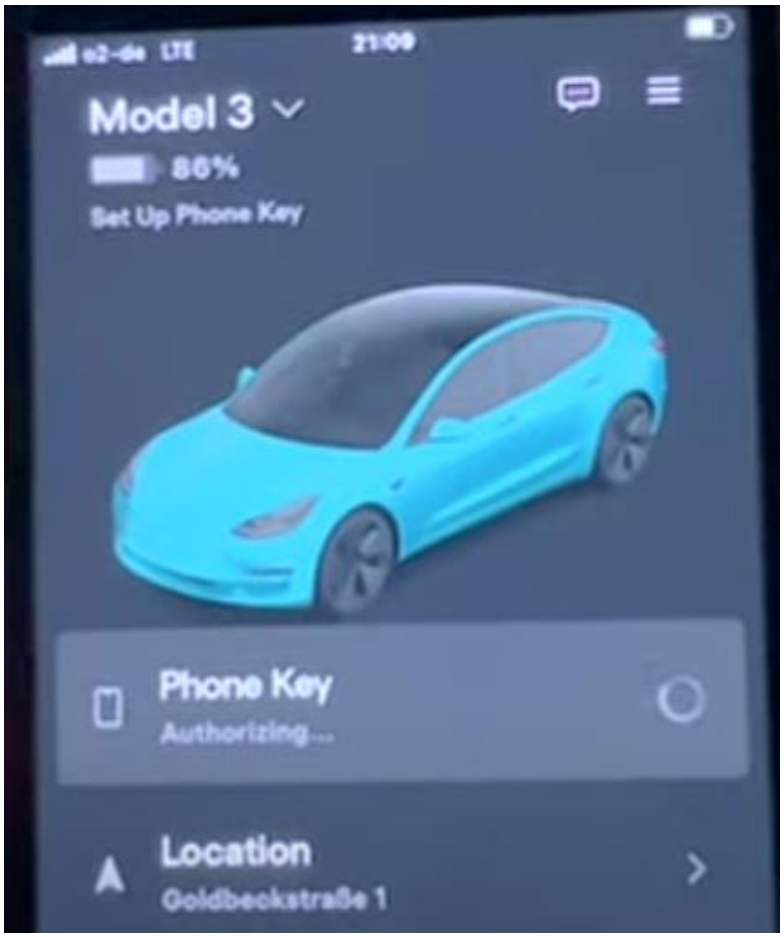


Figura 2 – Nova chave sendo adicionada.

Para dificultar a situação, uma vez adicionada uma nova Phone Key, o proprietário do Tesla não recebe uma notificação sobre o fato por meio do aplicativo e nenhum alerta é mostrado na tela sensível ao toque do carro. Com a nova Phone Key, o invasor pode destravar o carro e ativar todos os seus sistemas, permitindo que ele saia dirigindo como se fosse o proprietário.

Foi observado que o ataque foi bem-sucedido em um Tesla **Model 3**. No relatório à montadora, o pesquisador mostrou que a conta sequestrada deve pertencer ao motorista principal e que o veículo já deve estar vinculado a uma Phone Key. Argumentam também que exigir uma chave de cartão Tesla física ao adicionar uma nova chave de telefone melhoraria a segurança ao adicionar uma camada de autenticação para o novo telefone.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Bleepingcomputer**

heimdall
security research
A DIVISION OF ISH