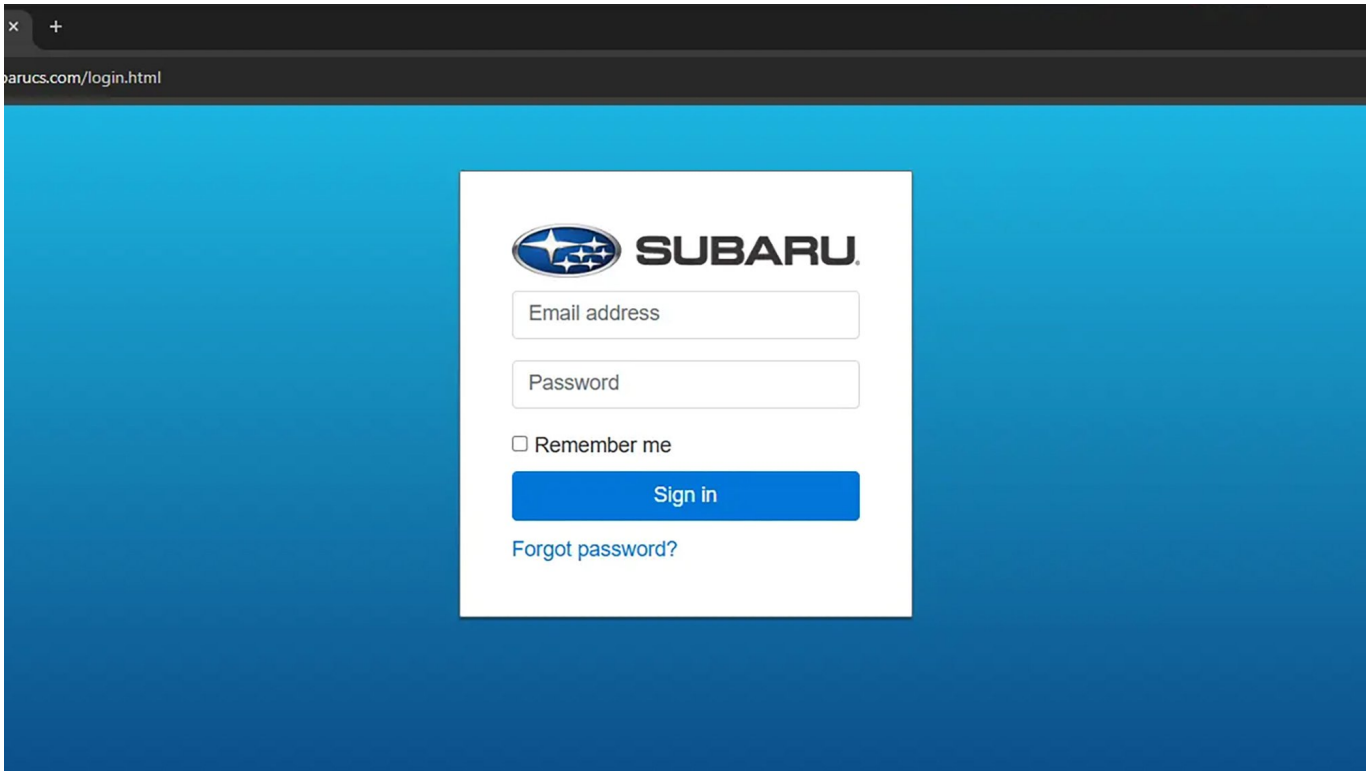
Sabemos que os carros estão melhor conectados do que nunca, o que é ótimo quando você quer se lembrar de onde você estacionou ou começa a descongelar as janelas do veículo enquanto você ainda está na cama – mas essa tecnologia moderna vem com preocupações com segurança e privacidade, como um novo Hack de carros Subaru e seu software Starlink mostrou.

Os pesquisadores de segurança Sam Curry e Shubham Shah explicam em um post de blog como foram capazes de invadir remotamente o serviço de veículo conectado ao Starlink, executado pela Subaru. Especificamente, eles direcionaram o software no carro da mãe de Curry, mas a mesma plataforma opera em veículos Subaru nos EUA, Canadá e Japão.

Com o acesso ao sobrenome do motorista e seu código postal anexo, endereço de e -mail, número de telefone ou placa, Curry e Shah puderam iniciar, parar, bloquear e desbloquear o Subaru, além de recuperar seu local atual. Além disso, eles poderiam ver o histórico de localização coletado por um ano inteiro (até os pontos de estacionamento).

O mesmo hack deu acesso a informações pessoais sobre o motorista, incluindo seu endereço, suas informações de cobrança (embora não o número completo do cartão de crédito) e o contato de emergência. O histórico de chamadas de suporte, as leituras do odômetro e os proprietários anteriores do motor também podem ser acessados.

Curry e Shah conseguiram testar o acesso a um Subaru pertencente a um de seus amigos, e funcionou novamente – tudo sem qualquer tipo de notificação ou alerta ao motorista do carro que seu veículo estava sendo acessado. Tudo o que era necessário foi um login bem - sucedido no portal Starlink e algumas informações básicas do driver.



O portal dos funcionários da Subaru foi alvo do hack.
Crédito: Sam Curry

Enquanto o login do Starlink foi protegido com autenticação de dois fatores e perguntas de segurança, essas medidas de segurança foram aplicadas de maneira sob medida que os pesquisadores conseguiram se locomover apenas modificando o código do site para ignorá-los. Em outras palavras, não havia necessidade de inserir uma senha.

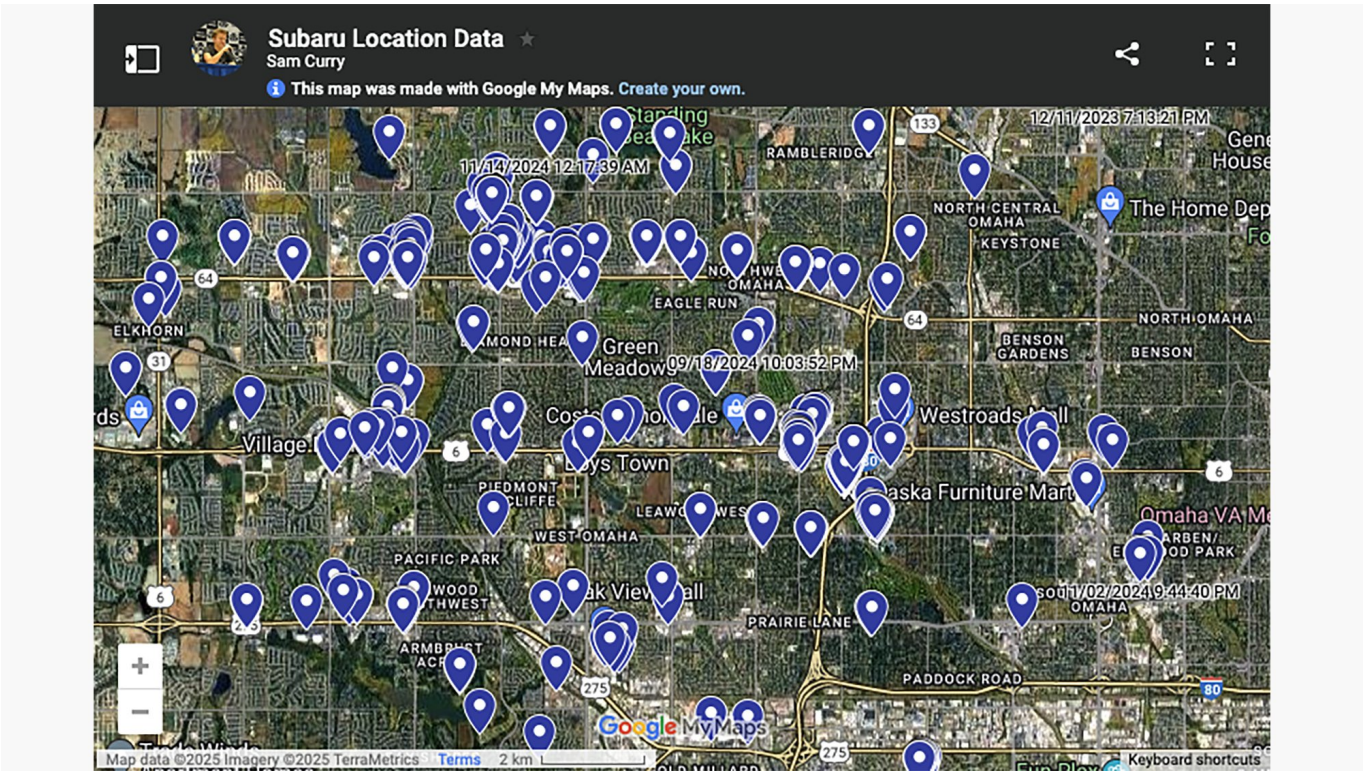
Essa é uma enorme quantidade de acesso a recursos e dados de um hack relativamente simples. A boa notícia é que Curry e Shah relataram a vulnerabilidade a Subaru, e o fabricante de veículos o remendou dentro de 24 horas – esse hack não é mais possível. No entanto, todos esses dados permanecem acessíveis aos funcionários da Subaru, o que levanta mais questões.

Subaru e seus dados

O hack original foi feito logando no terminal Starlink como funcionário da Subaru, por meio de algum trabalho de detetive no LinkedIn e um pouco de ajuste do código do site. Embora essa rota de acesso já tenha sido trancada, a equipe genuína da Subaru ainda pode obter todas as informações encontradas por Curry e Shah, incluindo o histórico de localização do ano.

“A indústria automobilística é única, pois um funcionário de 18 anos do Texas pode consultar as informações de cobrança de um veículo na Califórnia e não acertará nenhum

alarme”, escreve Curry. “Faz parte do trabalho diário normal. Todos os funcionários têm acesso a uma tonelada de informações pessoais, e a coisa toda depende da confiança”.



Os funcionários da Subaru podem ver onde você esteve via Starlink.
Crédito: Sam Curry

A Subaru disse à Wired que seus funcionários, “com base em sua relevância no trabalho”, podem acessar dados de localização – no caso de entrar em contato com os socorristas quando uma colisão é detectada, por exemplo (embora isso dificilmente exija um ano de dados). Os acordos de privacidade, segurança e NDA são assinados por esses funcionários, diz Subaru.

Você pode ler as políticas de privacidade da Subaru aqui e aqui. Você notará que há muitos dados coletados sobre você e seu veículo via Starlink, incluindo onde ele começa e para, velocidades do veículo e informações de diagnóstico. Use um site ou aplicativo Subaru e você permitir acesso a toda uma nova série de dados, incluindo dados coletados pelos microfones e câmeras em seus dispositivos.

Pior ainda, essas políticas se aplicam a qualquer passageiro em um Subaru – o desenvolvedor da Firefox Mozilla tem uma repartição abrangente aqui (observe que isso inclui os aplicativos e o site da Subaru e também como Starlink). Embora a Subaru promete não vender seus dados a terceiros e diz que exige que as informações melhorem o suporte e detectassem atividades criminosas, elas podem atingir você com anúncios, comunicações e promoções.

Os pesquisadores conseguiram obter muitos dados do usuário.
Crédito: Sam Curry

Existem etapas que você pode tomar para limitar parte dessa coleta de dados. É claro que você pode cancelar sua assinatura do Starlink, mas depois perde recursos como assistência de emergência. Você também pode desinstalar quaisquer aplicativos relacionados ao Subaru do seu telefone, alterar suas preferências de marketing pelo portal Mysubaru e preencher este formulário para colocar certos limites na coleta e compartilhamento de dados em estados específicos-embora não esteja claro quais dados o formulário cobre ou quanto tempo os dados existentes serão mantidos.

Subaru não está sozinho entre os fabricantes de carros quando se trata de vulnerabilidades de segurança e suspeitos de políticas de privacidade. No entanto, é outro lembrete de que a conectividade extra geralmente vem com um custo extra em termos de dados do usuário – e que qualquer decisão sobre qual carro comprar a seguir provavelmente deve vir com uma olhada nas políticas de coleta de dados do fabricante também.

function facebookPixelScript() { if (!facebookPixelLoaded) { facebookPixelLoaded = true; document.removeEventListener('scroll', facebookPixelScript); document.removeEventListener('mousemove', facebookPixelScript); window.zdconsent.cmd.push(function() { ! function(f, b, e, v, n, t, s) { if (f.fbq) return; n = f.fbq = function() { n.callMethod ? n.callMethod.apply(n, arguments) : n.queue.push(arguments) }; if (!f._fbq) f._fbq = n; n.push = n; n.loaded = !0; n.version =

'2.0'; n.queue = (); t = b.createElement(e); t.async = !0; t.src = v; s = b.getElementsByTagName(e)(0); s.parentNode.insertBefore(t, s) }(window, document, 'script', '//connect.facebook.net/en_US/fbevents.js'); fbq('init', '37418175030'); fbq('track', "PageView"); }); } }