Apple emite avisos de spyware enquanto CERT-FR confirma ataques

Data: 2025-09-12 08:51:57

Autor: Inteligência Against Invaders

Apple emite avisos de spyware enquanto CERT-FR confirma ataques

A Apple alertou os usuários sobre uma campanha de spyware; A agência cibernética da França confirmou que os dispositivos vinculados ao iCloud podem estar comprometidos.

A Apple alertou os clientes na semana passada sobre novos ataques de spyware, disse a Equipe Nacional de Resposta a Emergências de Computadores (CERT-FR). A agência confirmou pelo menos quatro desses alertas desde o início de 2025.

A Apple enviou alertas de spyware em 5 de março, 29 de abril, 25 de junho e 3 de setembro por e-mail, telefone e account.apple.com, onde os avisos também aparecem após o login.

“Receber uma notificação significa quepelo menos um dos dispositivos vinculados à conta do iCloud foi direcionado e está potencialmente comprometido. A notificação resulta no recebimento de um iMessage e um e-mail de alerta enviado pela Apple (de notificações de ameaças[at]email.apple.com ou notificações de ameaças[at]apple.com). Ao fazer login na conta do iCloud, um alerta é exibido. O tempo entre a tentativa de compromisso e o recebimento da notificação é de vários meses, mas permanece variável.” lê o relatório *publicado pela CERT-FR. “As notificações enviadas relatam ataques altamente sofisticados, a maioria dos quais emprega vulnerabilidades de dia zero ou não requer nenhuma interação do usuário.”*

Desde 2021, a Apple notifica pessoas visadas por spyware como Pégaso, Predador, Grafiteou Triangulação. Esses ataques atingem grupos de alto risco, como jornalistas, advogados, ativistas, políticos e executivos de setores estratégicos. Uma notificação sinaliza que pelo menos um dispositivo vinculado ao iCloud foi comprometido. A Apple envia alertas via iMessage, e-mail e login do iCloud, geralmente meses após a tentativa. O CERT-FR rastreia campanhas conhecidas, mas a lista não é exaustiva.

Se você receber um alerta da Apple, entre em contato com o CERT-FR, guarde o e-mail e não altere o dispositivo para preservar evidências. Para reduzir os riscos de spyware, atualize dispositivos, ative atualizações automáticas, separe o uso pessoal e profissional, use o Modo de Isolamento e reinicie diariamente. Pratique uma boa higiene de TI: evite links suspeitos, use códigos fortes, habilite 2FA e evite aplicativos não confiáveis.

O CERT-FR não compartilhou detalhes técnicos sobre os ataques direcionados aos usuários da Apple.

Siga-me no Twitter:**@securityaffairs**e**Linkedin**e**Mastodonte**

PierluigiPaganini

(Assuntos de Segurança–HackingCISA)