1 em cada 3 aplicativos Android vazam dados confidenciais - Against Inva

Data: 2025-09-19 02:44:42

Autor: Inteligência Against Invaders

Uma parcela significativa dos aplicativos móveis está expondo informações confidenciais por meio

de APIs inseguras, deixando usuários e empresas vulneráveis a ataques.

O *Relatório Global de Ameaças Móveis da Zimperium 2025,* publicado hoje, revelou que umem cada trêsAplicativos Android e mais da metade dos aplicativos iOS vazam dados que podem ser explorados.

Quase metade de todos os aplicativos ainda contém segredos codificados, como chaves de API, que permitem que os invasores façam engenharia reversa e os usem indevidamente depois que os aplicativos são publicados.

Aplicativos móveis como uma superfície de ataque crescente

O relatório descobriu que as fraquezas do lado do cliente estão alimentando novos caminhos para o abuso. Os invasores podem adulterar aplicativos, interceptar tráfego e explorar dispositivos comprometidos para contornar as defesas.

Outras descobertas importantes incluem:

- 1 em cada 400 dispositivos Android está enraizado e 1 em 2500 dispositivos iOS está desbloqueado
- 3 em cada 1000 dispositivos móveis já estão comprometidos
- 1 em cada 5 dispositivos Android encontra malware na natureza
- Quase 1 em cada 3 aplicativos financeiros Android e 1 em cada 5 aplicativos de viagem iOS permanecem abertos a ataques man-in-the-middle, apesar da fixação SSL

“Os aplicativos móveis não consomem apenas APIs, eles as expõem”, afirmou o relatório.

“Sem visibilidade do aplicativo e do dispositivo que faz a chamada, os invasores podem […] Mapear e manipular o comportamento da API modificando o código do aplicativo […] Extraia segredos e tokens fazendo engenharia reversa do aplicativo [and] explorar controles no nível do dispositivo para simular o uso real.”

Leia mais sobre os riscos de segurança da API: 99% das organizações relatam problemas de segurança relacionados à API

Defesas de perímetro não são suficientes

Ferramentas tradicionais, como firewalls, gateways de API e firewalls de aplicativos Web, podem bloquear determinadas ameaças no perímetro, mas não podem determinar se o tráfego é originado de um aplicativo genuíno ou de um clone adulterado. Esse ponto cego permite que os invasores falsifiquem identificadores de identidade, localização e dispositivo, fazendo com que as chamadas de API maliciosas pareçam legítimas.

“Do ponto de vista da segurança, precisamos garantir que os dispositivos móveis tenham proteções básicas, não apenas para a organização, mas também para os próprios usuários”, disse Randolph Barr, CISO da Cequence Security.

“No mínimo, isso significa garantir que um bloqueio de tela esteja ativado, as atualizações sejam aplicadas em tempo hábil e que os dispositivos não sejam enraizados ou desbloqueados.”

Fechando as lacunas

O relatório da Zimperium enfatizou que a proteção das APIs deve começar dentro do próprio aplicativo móvel. Salientou duas abordagens essenciais:

- Um**Endurecimento PI**: Protegendo endpoints, tokens e lógica de negócios com ofuscação, armazenamento seguro e defesas de tempo de execução
- **Atestado de aplicativo**: Validar se cada chamada de API vem de um aplicativo genuíno e não adulterado em execução em um ambiente confiável

“Hoje, estamos enfrentando uma realidade preocupante: muitos aplicativos móveis corporativos ainda carecem de proteções básicas, como ofuscação de código, armazenamento seguro e bibliotecas de terceiros atualizadas”, explicou Vishrut Iyengar, gerente sênior de soluções da Black Duck.

“Essas fraquezas permanecem exploráveis mesmo em ambientes corporativos gerenciados.”

David Matalon, CEO da Venn, ecoou as opiniões de Iyengar: “O perímetro tradicional se foi, e a

realidade do Bring Your-Own-Device para trabalhadores remotos requer uma mudança de estratégia: de proteger o dispositivo para proteger o trabalho em si”.