Os aplicativos móveis do seu celular são a nova porta de entrada para ciberataques cada vez mais sofisticados?

*Pesquisa mostra que o Brasil é o quinto país mais alvo de ataques cibernéticos no mundo e os ataques móveis estão crescendo em sofisticação*

Devido à sua crescente popularidade e à sensibilidade dos dados neles armazenados, os aplicativos móveis são um alvo cada vez mais atraente para os hackers. E por definição, os aplicativos móveis são extremamente vulneráveis porque são executados em ambientes desprotegidos, fora do datacenter e dos firewalls, deixando-os sujeitos a uma ampla variedade de tipos diferentes de ameaças e ataques.

Dados confidenciais armazenados no dispositivo ou usados pelo aplicativo ou usuário podem ser facilmente comprometidos usando centenas de ferramentas poderosas, disponíveis gratuitamente e fáceis de usar, que abrem milhares de vetores de ameaças exploráveis exclusivos para dispositivos móveis.

Segundo pesquisa recente da Kaspersky, o Brasil é o quinto país mais visado, com 1,2 milhão de ataques cibernéticos em todo o mundo. “Os aplicativos móveis são vulneráveis a várias formas de ataques cibernéticos e podem, de fato, ser hackeados. Os cibercriminosos podem explorar falhas de segurança até mesmo em aplicativos. É por isso que a segurança de aplicativos móveis não deve ser negligenciada”, explica Tom Tovar, CEO e cofundador da Appdome, o one-stop para defesa de aplicativos móveis.

Para entender melhor o problema, Appdome, pioneira em segurança automatizada de aplicativos móveis, explica como os aplicativos móveis modernos se tornaram o novo terreno fértil para os criminosos cibernéticos explorarem por meio de campanhas de fraude extremamente sofisticadas e escaláveis, ao mesmo tempo que passam despercebidas às soluções de segurança tradicionais.

**Phishing móvel e fraude sintética**

O phishing é um método de ataque antigo há décadas e vem em muitas variedades. Em um

ataque de phishing, a vítima recebe um convite para interagir com um conteúdo falso ou malicioso que imita uma entidade confiável, como uma mensagem do seu banco solicitando que você verifique sua conta adicionando seu número de seguro social. A vítima pensa que está enviando informações confidenciais para seu banco, mas na verdade as está enviando para um malware ou invasor.

Historicamente, o e-mail tem sido um canal popular através do qual são conduzidas campanhas de phishing, mas não é o único. Na verdade, os ataques de phishing modernos vão muito além do e-mail e muitas vezes envolvem aplicativos móveis armados, usando métodos de ataque sofisticados, como malware de sobreposição, malware de serviço de acessibilidade, aplicativos e clones falsos, cavalos de Tróia com malware ofuscado ou criptografado e muito mais.

**Malware, ataques de sobreposição e cavalos de Tróia**

O malware, um tipo de software malicioso projetado para se infiltrar, danificar ou comprometer aplicativos, pode se infiltrar em aplicativos ou sistemas infectados. Eles podem roubar informações e monitorar atividades, sendo devastadores para a segurança do usuário.

Por exemplo, tomemos como exemplos os trojans bancários BrasDex e Xenomorph, que abusam dos recursos do Android Accessibility Service para interceptar eventos entre o sistema operacional e o aplicativo. Em seguida, ele aproveita uma carga de malware especializada chamada “ATS” ou Sistema de Transferência Automatizada, permitindo inserir informações em campos dentro do aplicativo móvel. Isso permite que o trojan se disfarce como usuário de banco móvel, contorne a MFA e conclua transações de ponta a ponta, como transferências de dinheiro – tudo sem o conhecimento ou envolvimento do usuário.

**Bots maliciosos e ataques de botnets**

Os bots maliciosos, muitas vezes chamados de “bots ruins”, são programas automatizados

projetados para realizar ações prejudiciais ou enganosas, como fraude, coleta de dados e roubo financeiro. Esses bots estão crescendo em sofisticação, imitando o comportamento humano e explorando atividades legítimas de aplicativos móveis, tornando-os difíceis de detectar. As soluções anti-bot tradicionais foram projetadas para aplicações web e não possuem inteligência para detectar explorações direcionadas a aplicações móveis ou ao canal móvel, o que deixa um enorme ponto cego na estratégia de proteção da maioria das organizações.

**A mudança de responsabilidade: um apelo aos desenvolvedores**

À luz do cenário de ameaças móveis em constante evolução, os utilizadores encontram-se numa posição precária, enfrentando a natureza sofisticada dos ataques cibernéticos modernos.

“Os usuários podem garantir que possuem senhas complexas e baixar aplicativos móveis apenas de lojas de aplicativos oficiais. Todo mundo já ouviu esse conselho antes, mas a verdade é que a segurança não deve depender apenas do usuário. A verdade é que é responsabilidade dos desenvolvedores. Reconhecendo esta realidade, as agências governamentais reconheceram esta mudança crucial de responsabilidade”, explica Tovar.

Um exemplo é a estratégia de cibersegurança de Kamala Harris e Joe Biden nos EUA, que sublinha a necessidade dos programadores e proprietários de tecnologia assumirem um papel proativo na segurança das suas aplicações móveis.

A indústria deve priorizar as proteções nos aplicativos, já que os usuários móveis dependem cada vez mais dos desenvolvedores para fortalecer seus aplicativos contra ameaças emergentes. Governos de todo o mundo também estão tomando medidas específicas para responsabilizar os fabricantes de aplicativos móveis pela proteção dos usuários contra fraudes e malwares móveis, deixando claro que os desenvolvedores devem criar proteções robustas nos aplicativos como parte de uma defesa de segurança em várias camadas, a fim de tornar os aplicativos resiliente à natureza cada vez mais sofisticada e dinâmica das

Os aplicativos móveis do seu celular são a nova porta de entrada para ciberataques cada vez mais sofisticados?

ameaças cibernéticas modernas.

Empresas como a Appdome estão inaugurando uma nova maneira de proteger aplicativos móveis, usuários e empresas, aproveitando a automação. Isso permite que as equipes de desenvolvimento e cibernéticas usem inteligência abrangente sobre ameaças e dados de ataque em tempo real em aplicativos móveis de produção para tomar decisões informadas sobre quais proteções construir em aplicativos Android e iOS.

Em seguida, eles usam a mesma plataforma de automação de defesa cibernética sem código para fornecer essas proteções diretamente em aplicativos móveis em minutos, diretamente de seu pipeline de CI/CD existente que já usam para criar e fornecer novos aplicativos e recursos.

“À medida que a tecnologia móvel avança, também deve avançar a nossa abordagem à segurança. Os utilizadores não estão indefesos, mas o fardo da proteção deve transferir-se legitimamente para os programadores que criam as experiências digitais em que confiamos. Ao abraçar esta mudança de paradigma, a indústria móvel pode promover um ambiente mais seguro, garantindo que os utilizadores possam confiar na segurança das suas interações digitais”, conclui Tovar.

**Sobre a Appdome**

Appdome, o one-stop shop para defesa de aplicativos móveis, está em uma missão para proteger todos os aplicativos móveis do mundo e as pessoas que usam aplicativos móveis em suas vidas e no trabalho. A Appdome fornece a única plataforma de automação de defesa cibernética para aplicativos móveis do setor, equipada com mecanismo de codificação baseado em inteligência artificial patenteado, Threat-Events™ Threat-Aware UX/UI Control e ThreatScope™ Mobile XDR. Usando a Appdome, as marcas móveis eliminam a complexidade, economizam dinheiro e oferecem mais de 300 certificados de segurança de aplicativos móveis Secure™, antimalware, antifraude, antibot móvel, antitrapaça, prevenção de ataque MiTM, ofuscação de código e outras proteções no Android e aplicativos iOS com facilidade,

dentro do DevOps móvel e do pipeline de CI/CD. As principais marcas financeiras, de saúde, governamentais e de comércio eletrônico usam o Appdome para proteger aplicativos Android e iOS, clientes móveis e negócios móveis em todo o mundo. A Appdome detém várias patentes, incluindo as patentes dos EUA 9.934.017 B2, 10.310.870 B2, 10.606.582 B2, 11.243.748 B2 e 11.294.663 B2. Patentes adicionais pendentes