Resumo de solução

Proteção contra conluio de aplicativos móveis

Os aplicativos móveis de hoje precisam de uma maneira conveniente de se comunicarem uns com os outros. Infelizmente, esses úteis canais de comunicação também podem esconder comportamentos insidiosos. Quando dois ou mais aplicativos são analisados independentemente, o comportamento de um único aplicativo pode parecer completamente inofensivo. Porém, quando aplicativos móveis capazes de trabalhar em conluio são instalados no mesmo dispositivo, eles podem trocar informações e realizar atos maliciosos.

No *Relatório do McAfee Labs sobre ameaças: junho de 2016*, examinamos em profundidade o conluio de aplicativos móveis, um novo método que os aplicativos maliciosos utilizam para dificultar a detecção. Por questão de segurança, os sistemas operacionais móveis isolam seus aplicativos em áreas restritas (sandboxes), restringem suas capacidades e controlam claramente suas permissões. Contudo, os sistemas operacionais móveis também incluem muitas maneiras pelas quais esses aplicativos podem se comunicar e trocar informações uns com os outros, ultrapassando limites de sandbox.

Procurando evitar detecções, os atacantes podem tentar se aproveitar de vários aplicativos com diversas capacidades e permissões para alcançar seus objetivos. Por exemplo, digamos que o aplicativo A tem permissão para informações confidenciais, enquanto o aplicativo B tem acesso à Internet. Quando cada aplicativo é instalado individualmente, o aplicativo A não pode enviar essas informações para fora do dispositivo e o dispositivo B não tem acesso às informações confidenciais. Mas quando estão instalados no mesmo dispositivo, o aplicativo A pode enviar as informações confidenciais para o aplicativo B, o qual, por sua vez, pode enviar as informações para um destino externo.

O conluio de aplicativos móveis permite que os aplicativos evitem detecções ao desempenhar comportamentos maliciosos como:

- **Roubo de informações:** quando um aplicativo com acesso a informações sigilosas ou confidenciais colabora (deliberadamente ou não) com um ou mais outros aplicativos para enviar informações para fora do dispositivo.
- **Roubo financeiro:** quando um aplicativo envia informações para outro aplicativo capaz de realizar transações financeiras ou chamadas de API financeira.

intel Security

- **Uso abusivo do serviço:** quando um aplicativo pode controlar um serviço de sistema e receber informações ou comandos de um ou mais aplicativos.
- **Elevação de privilégios:** quando um aplicativo oferece seus privilégios elevados a outros aplicativos para coleta de dados confidenciais ou execução de ações nocivas.

Proteção contra conluio de aplicativos móveis

A Intel® Security tem diversas práticas recomendadas para proteção contra aplicativos móveis em conluio:

- **Use aplicativos de fornecedores e lojas de aplicativos confiáveis** porque fontes autorizadas realizam varreduras de rotina em busca de malware em seus aplicativos listados.
- **Desative a capacidade de instalar aplicativos de "fontes desconhecidas"** para evitar a instalação de aplicativos que não tenham sido autorizados.
- **Evite utilizar software que contenha anúncios** porque o excesso de anúncios pode indicar a presença de múltiplas bibliotecas de anúncios, as quais aumentam a possibilidade de conluio.
- **Pesquise as avaliações e testes de um aplicativo antes de instalá-lo** para saber se outros usuários tiveram problemas de segurança com o aplicativo.
- **Não faça "jailbreak" ou "root" no dispositivo**, pois isso dá aos aplicativos acesso em nível de sistema e permite que instalem software malicioso.
- **Distribua uma solução de gerenciamento móvel** como mecanismo para controlar quais aplicativos os usuários podem instalar.

Como a Intel Security pode ajudá-lo a se proteger contra o conluio de aplicativos móveis

McAfee® Mobile Security for Android

Enquanto você faz download de novos aplicativos, navega na Internet ou realiza transações bancárias on-line, o McAfee Mobile Security for Android protege o seu dispositivo móvel contra ameaças. O McAfee Mobile Security for Android utiliza informações fornecidas por pesquisadores de ameaças do McAfee Labs para identificar aplicativos maliciosos, incluindo aplicativos móveis em conluio, e impede que os mesmos sejam executados no seu dispositivo móvel. Com o McAfee Mobile Security for Android, o seu dispositivo móvel fica protegido e pode utilizar qualquer aplicativo ou combinação de aplicativos com confiança.

O McAfee Mobile Security for Android oferece os seguintes recursos:

- Faz varreduras em tempo real para examinar automaticamente e-mails, mensagens de texto, anexos e arquivos quanto à presença de conteúdo malicioso.
- Realiza varreduras completas programadas com o Smart Scheduler.
- Possibilita atualizações automáticas para assegurar que as informações mais recentes dos pesquisadores de ameaças protejam você contra todos os tipos de ameaça, incluindo aplicativos móveis em conluio.
- Gera relatórios e alertas automaticamente, caso algum aplicativo cometa uma violação de privacidade, e permite que você desinstale aplicativos inseguros.
- Bloqueia sites arriscados que possam conter ameaças maliciosas.

Leitura adicional

Towards Automated Android App Collusion Detection (Rumo à detecção automatizada de conluio de aplicativos para Android), um relatório de pesquisa desenvolvido conjuntamente pelo McAfee Labs e por pesquisadores de diversas universidades do Reino Unido.

Colluding Apps: Tomorrow's Mobile Malware Threat (Aplicativos em conluio: a ameaça do malware móvel de amanhã), um artigo da revista IEEE Security & Privacy.

Analysis of the Communication Between Colluding Applications on Modern Smartphones (Análise da comunicação entre aplicativos em conluio em smartphones modernos), minuta da 28ª conferência anual de aplicativos de segurança para computadores.

A Survey on Application Collusion Attacks on Android Permission-Mechanism (Pesquisa sobre ataques de conluio de aplicativos contra o mecanismo de permissões do Android), International Journal for Scientific Research & Development.

Towards a Systematic Study of the Covert Channel Attacks in Smartphones (Rumo a um estudo sistemático dos canais de ataque dissimulado em smartphones), International Conference on Security and Privacy in Communication Networks.

Automatic Detection of Inter-Application Permission Leaks in Android Applications (Detecção automática de vazamentos de permissões entre aplicativos para Android), IBM Journal of Research and Development.

McAfee. Part of Intel Security.
Av. das Nações Unidas, 8.501 - 16º andar
CEP 05425-070, São Paulo - SP, Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com