Os cinco principais malwares móveis de 2012

Ameaças têm, em comum, sistema operacional Android. Pesquisa mostra crescente sofisticação dos cibercriminosos

Apesar da quantidade de softwares maliciosos com foco em dispositivos móveis ainda ser irrisória perto do total que visa os PCs, invasores cada vez mais têm como foco os dispositivos que os consumidores levam sem seus bolsos.

Até agora, vários malwares apareceram no radar e revelaram a crescente sofisticação dos cibercriminosos. Aqui está a lista dos cinco mais perigosos, sofisticados e prolíferos que apareceram até agora, em 2012. O que eles têm em comum? O sistema operacional Android.

1. Troia FakeInst SMS e seus variantes

"O FakeInst se disfarça de um app popular, como o Instagram, Opera Browser e Skype, e envia uma mensagem SMS para números sob taxa premium", afirmou Jerry Yag, vice-presidente de engenharia na empresa móvel de segurança TrustGo. "Foi selecionado porque é superinfeccioso. Há muitas variantes na família, como o RuWapFraud, Depositmobi, Opfake e JiFake. Sessenta por cento dos malwares Androids que descobrimos pertencem à família FakeInst. Seu local de ataque principal é a Rússia, mas também há amostras descobertas em todo o mundo".

2. SMSZombie

Também na lista está o SMSZombie, que foi recentemente descoberto em mercados terceirizados na China e infectou mais de 500 mil dispositivos. O malware funciona enviando mensagens SMS para sistemas de pagamento online da China Mobile e "cobrando das contas designadas", explicou Yang. "A quantidade de pagamentos, frequência e destino são todas controladas pelo desenvolvedor do malware. Ele tem significância porque é preciso cuidado extra para se proteger". Uma vez instalado, ele obtém privilégios Device Admin (API de administração de dispositivo; N. da T.), e é muito difícil de remover, o que levou a empresa TrustGo a publicar detalhes do processo de remoção manual em seu blog."Esperamos que mais malwares Android adotem técnicas similares para se protegerem."

3. NotCompatible

Descoberto pela Lookout Mobile Security em abril, o NotCompatible é a primeira peça de um malware móvel que usa sites como método de distribuição orientada, afirmou Derek Halliday, gerente de segurança de produto da Lookout. "O NotCompatible é baixado automaticamente quando o navegador do Android visita um site infectado. O aplicativo baixado é disfarçado como uma atualização de segurança numa tentativa de convencer o usuário a instalá-lo". Quando instalado com sucesso, o malware pode ser usado para ganho de acesso às redes privadas ao transformar o dispositivo Android infectado em um rede proxy, e pode com isso ter acesso à informação ou sistemas protegidos.

4. Android.Bmaster

Incorporado em aplicativos legítimos, o Android.Bmaster foi visto em um app market Android terceirizado no começo deste ano. A maioria das vítimas infectadas foi de usuários chineses. Uma vez no dispositivo, o malware rouba dados sensíveis do telefone, incluindo a ID do celular, código de área e número Imei (International Mobile Equipment Identity), o que leva ao envio de mensagens para números premiuns. "A análise dos servidores command-and-control do Android.Bmaster indicou que o número total de dispositivos infectados conectados ao botnet é de centenas de milhares", afirmou Kevin Haley, diretor da Symantec Security Response. "O número de dispositivos infectados e que podem gerar receita ficam entre 10 mil e 30 mil diariamente, o suficiente para render milhões de dólares ao invasor anualmente, se as taxas de infecção se mantiverem".

5. LuckyCat

LuckyCat foi o nome dado à campanha de ataques orientados que atingiram as indústrias aeroespaciais e de energia no Japão, ativistas tibetanos e outros. Para ampliar o ataque, invasores o levaram para a plataforma Android. Uma vez instalado, o aplicativo mostra um ícone preto com o texto "testService" e abre uma backdoor (falha de segurança; N. da T.) no dispositivo para roubar informações.

"Este é a primeira APT [advanced persiten threat] orientado à plataforma Android. É um cavalo de troia que abre uma backdoor e rouba informações nos dispositivos infectados", finalizou Yang, da TrustGo.

Fonte: Itweb [Portal]. Disponível em: <http://itweb.com.br/61634/os-cinco-principais-malwares-moveis-de-2012/>. Acesso em: 2 out. 2012.