ENJOY SAFER TECHNOLOGY™

GUIA DE SEGURANÇA PARA

Smartphones

Introdução

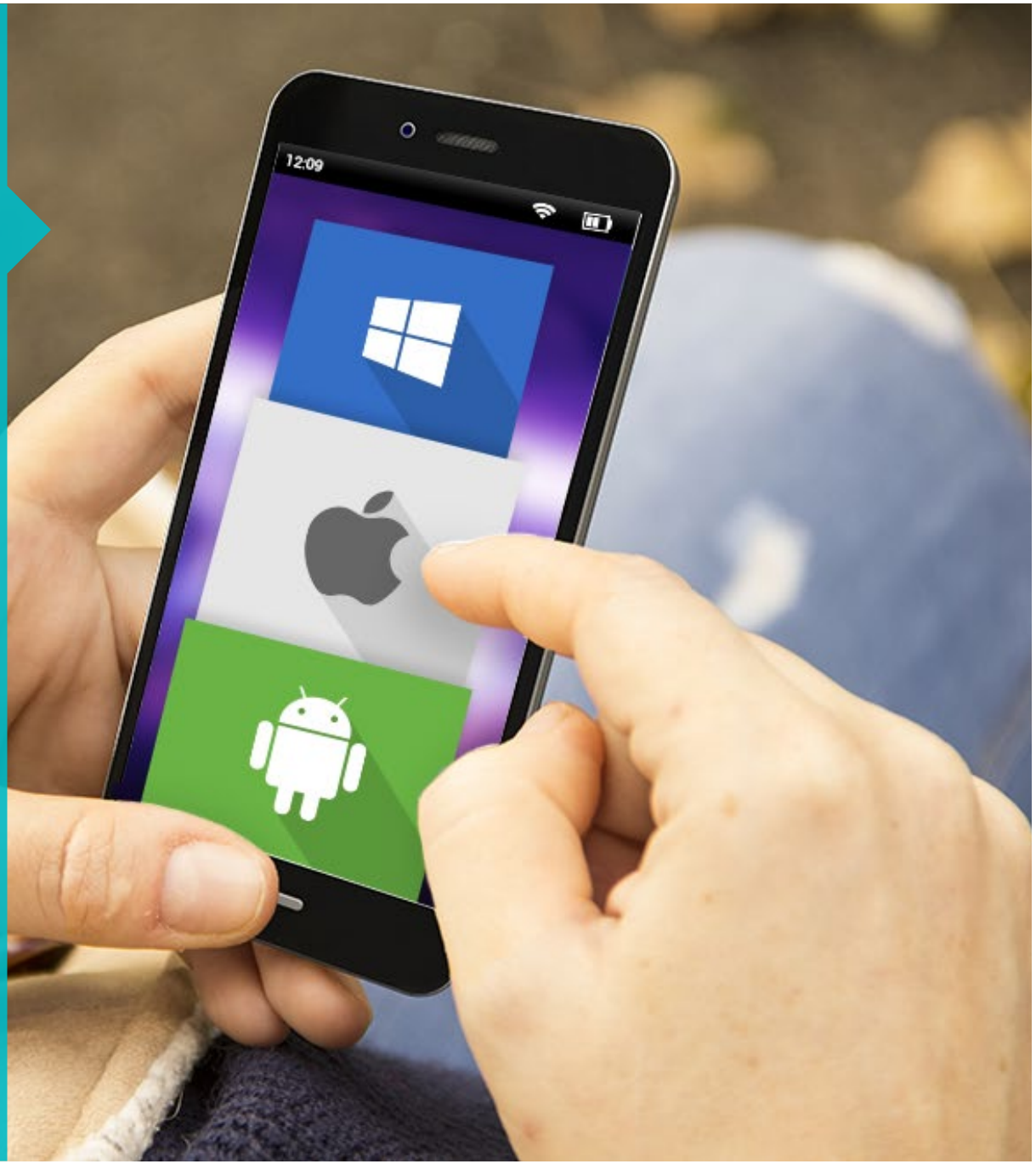
Com o passar dos anos, os telefones celulares experimentaram uma intensa evolução e incorporaram novas capacidades e serviços. Neles, os usuários armazenam cada vez mais informação pessoal e sensível que, além de estar exposta ao furto ou extravio do dispositivo, pode ser valiosa para os cibercriminosos que buscam obter ganhos ilícitos utilizando códigos maliciosos ou outras ameaças.

Nem todos os sistemas operacionais do mercado móvel são atacados de maneira igual por códigos maliciosos. Existem recomendações gerais que se aplicam a todo tipo de caso, dispositivo –smartphones, tablets ou similares – e usuários.

Quais são as principais ameaças que afetam os dispositivos móveis? Quais medidas podem ser adotadas para mitigar o impacto destes ataques? Através das respostas a estas perguntas, os usuários poderão fazer uso seguro e consciente de seus dispositivos móveis.

Índice

Sistemas operacionais móveis



Sistemas operacionais móveis

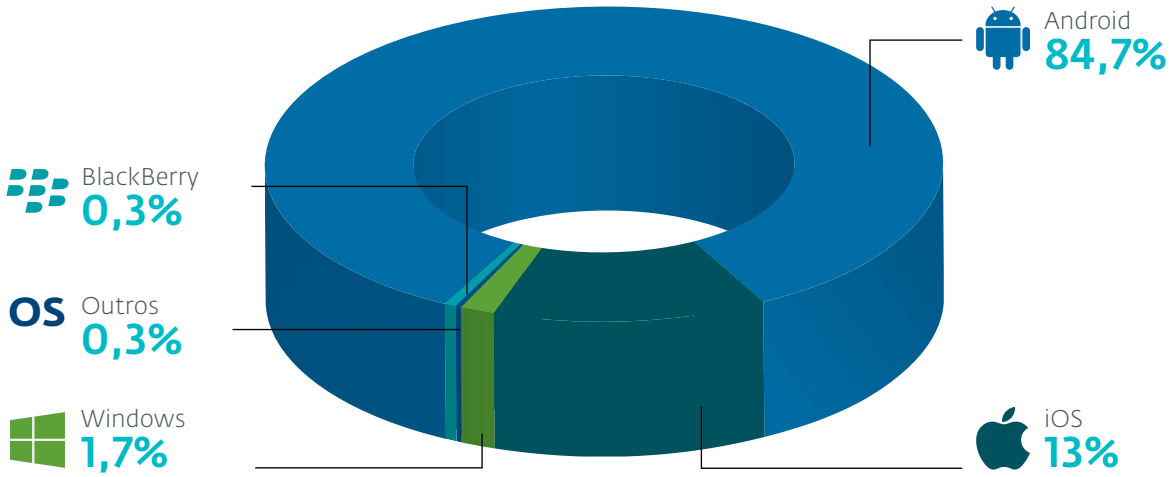
Igual aos computadores que possuem vários sistemas operacionais, os smartphones também precisam de um para funcionar. Atualmente, existem diversas opções dentro do mercado: Android, iOS, Windows Phone, Symbian, BlackBerry, entre outros.

Percentual mundial de uso de cada sistema operacional móvel

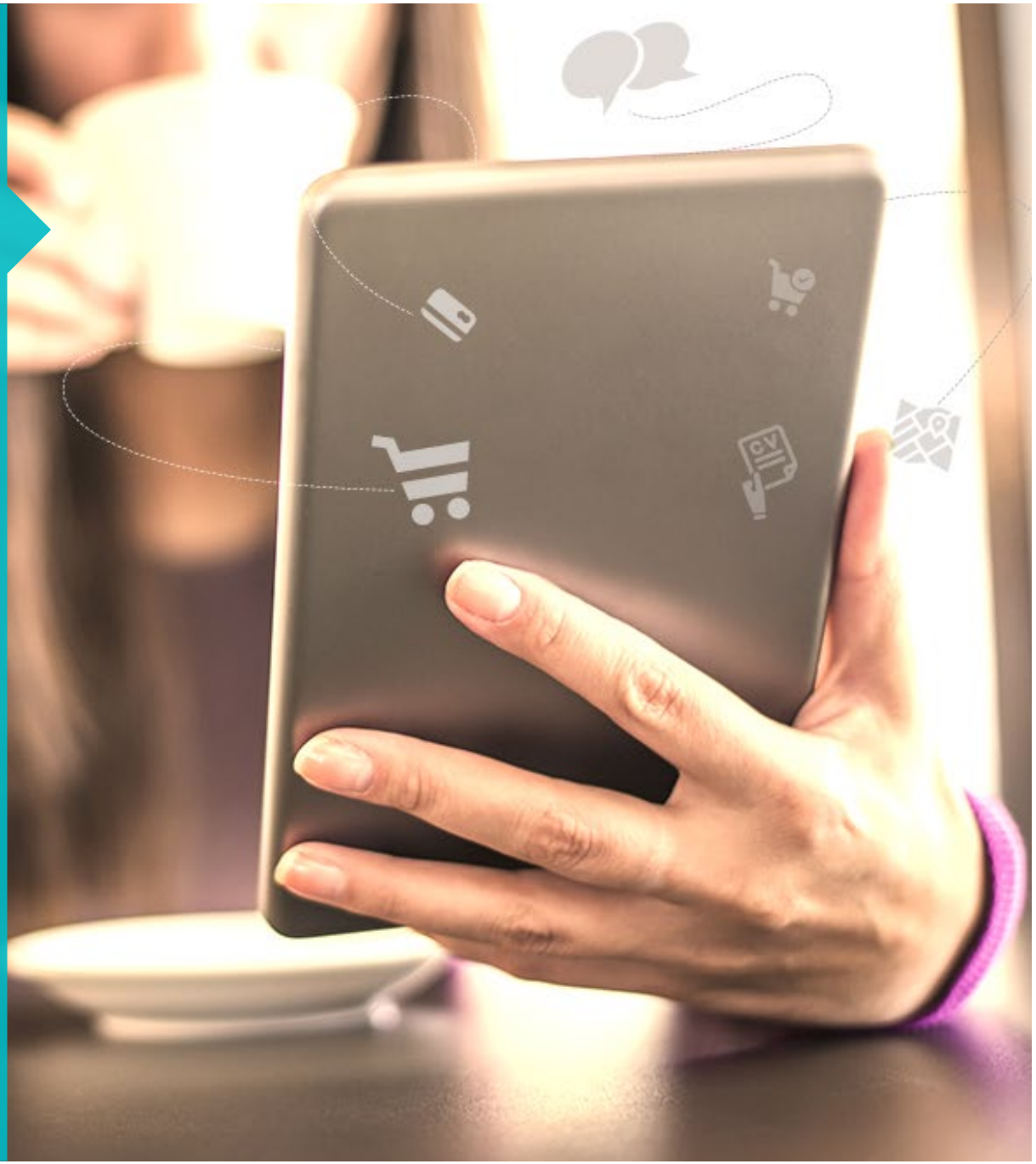
Existem muitas ameaças latentes no mundo móvel. Em particular, a maior parte do mercado é tomado por dois únicos gigantes: Android e iOS. Como é de se imaginar, os cibercriminosos têm isso em mente quando decidem gerar campanhas de propagação de códigos maliciosos. É por isso que estas duas plataformas são alvos exclusivos para a grande variedade de ameaças móveis.

Segundo a consultoria **Gartner**, o sistema operacional móvel com maior taxa de participação de mercado é o Android. Devido à massividade e abertura do mesmo, é possível observar que a maioria dos códigos maliciosos para celular que se desenvolvem na atualidade estão destinados a esta plataforma e seus usuários.

No Laboratório de Análises de Malware da ESET América Latina foram detectados códigos maliciosos para Android capazes de subtrair informação sensível da vítima, rastreá-la através de GPS, transformar o dispositivo móvel em parte de um **botnet**, infectar o terminal com **ransomware**, entre outras ações maliciosas.



Riscos associados ao uso destes dispositivos



Riscos associados ao uso destes dispositivos

Enquanto que os telefones celulares concentram cada vez mais serviços encarregados de processar informação sensível, os dados que eles gerenciam incrementam seu valor aos olhos dos cibercriminosos. Na atualidade, existem diversos tipos de ataques e/ou riscos que podem afetar os usuários de smartphones, a saber: malware, exploração de vulnerabilidades, phishing, fraudes e roubo ou perda do dispositivo. Cada um destes riscos pode prejudicar o usuário de diferentes maneiras.

Os telefones móveis são equipamentos muito pessoais. Através deles, se manipulam dados privados, como informação de cartão de crédito, compras, dados de contatos próximos, vídeos e fotografias, itinerários, geolocalização, arquivos e seus metadados, históricos de sites visitados, conexões Wi-Fi realizadas, chaves de acesso a serviços de e-mail e outros serviços na nuvem, mensagens de texto e conversas em múltiplas redes sociais, entre muitas outras coisas.

Todos estes dados armazenados podem ser úteis para que um cibercriminoso orqueste um ataque com técnicas de Engenharia Social contra o dono do terminal. O fato desta informação cair em mãos erradas pode derivar, inclusive, em casos de extorsão e fraude ante a ameaça de exposição destes dados.

Não é menos preocupante a possibilidade de que estranhos possam acessar as contas de aplicativos pessoais ativas no dispositivo, como redes sociais, plataformas de compra online ou serviços bancários. Por isso, é fundamental adotar medidas preventivas para proteger-se ante estes riscos.

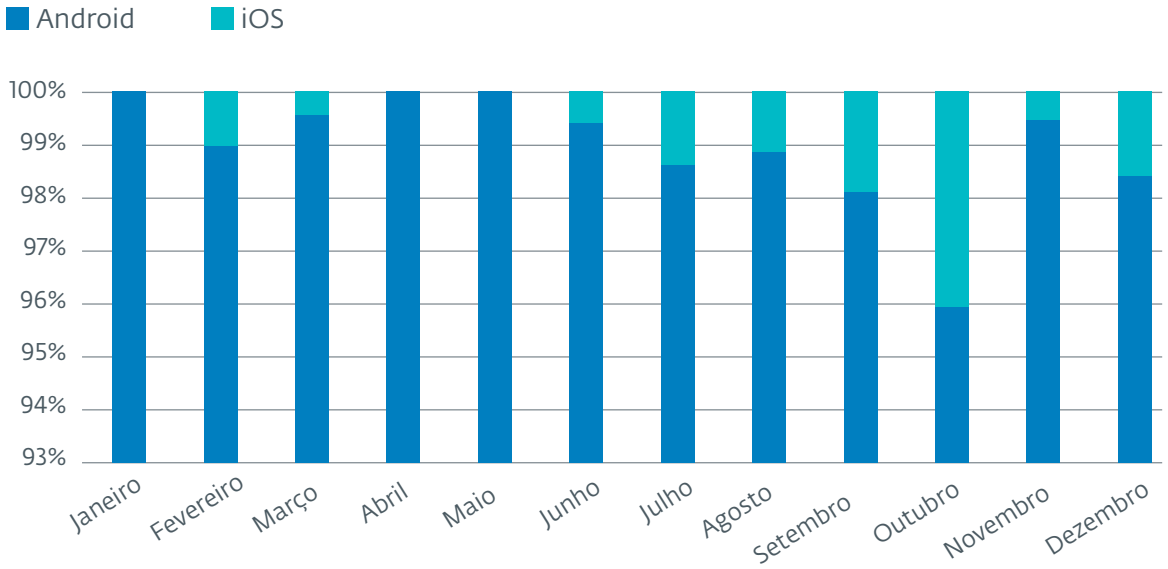
O malware e os smartphones

O malware e os smartphones

Ainda que há alguns anos a problemática dos códigos maliciosos afetasse predominantemente os computadores, atualmente também representa um risco para os usuários de smartphones. Assim, a maioria das famílias de códigos maliciosos móveis tem como objetivo a assinatura de serviços SMS Premium, o roubo de informação, o sequestro do terminal ou seus dados, a instalação de outras ameaças no sistema ou o controle remoto do equipamento.

Em geral, o êxito na propagação de qualquer tipo de ameaça informática – com exceção da perda ou roubo do telefone – se apoia principalmente nas estratégias de Engenharia Social que o cibercriminoso utiliza. Usualmente, as vítimas são enganadas com promessas de jogos para celular, novas versões de apps para redes sociais ou mensagens, programas para o rooting ou jailbreaking do telefone ou repositórios de downloads não oficiais.

Novas variáveis de malware em 2015



Códigos maliciosos no Android

No que diz respeito ao Android, a taxa de detecção de novas amostras maliciosas é de, em média, duzentas mensais. Dentro das famílias que tiveram maior crescimento, o malware dedicado ao envio de mensagens SMS a números Premium, o spyware e o r**ansomware móvel** são as que ocupam os primeiros lugares da lista.

Esta tendência é preocupante, posto que se trata de códigos que têm consequências sumamente prejudiciais para os donos dos terminais: perda de informação sensível, inutilização dos dispositivos e verdadeiros gastos econômicos.

Ao longo de 2015, se observaram novas amostras que causaram estragos em nível global. Uma delas foi o **Android/Lockerpin:** um agressivo **ransomware para Android capaz de mudar o código PIN do equipamento e inutilizá-lo.**

Talvez o mais curioso do ano tenha sido o descobrimento de malware em plataformas oficiais para distribuição de aplicativos. **Variáveis de scareware disponíveis na Play Store,** disfarçados de truques para o popular jogo Minecraft com mais de 600 mil usuários infectados, **phishing orientado a roubar credenciais do Facebook** instalado mais de 500 mil vezes ou cerca de cinquenta **trojans por cliques de sites pornográficos.**

Códigos maliciosos em iOS

O debate acerca das diferenças entre os esquemas de segurança de iOS e Android, suas vantagens e desvantagens, parece que nunca terá um final. Não obstante, é certo que muitos usuários de iOS descuidam de sua segurança por terem certeza de que não existem códigos maliciosos dirigidos a este sistema operacional.

Ainda que a quantidade de malware conhecido para iOS continua representando percentuais menores quando em contraste com a enorme diversidade de malware para Android, a incidência de códigos maliciosos nesta plataforma é inegável.

Neste sentido, é possível lembrar do **XCodeGhost**, um dos contratempos que a Apple sofreu em matéria de segurança móvel e que os levou a remover mais de 300 aplicativos infectados com malware de sua App Store, logo que se confirmou um incidente em sua segurança.

Pouco depois deste fato, investigadores encontraram outros **256 aplicativos que violavam a política de privacidade da App Store,** que proíbe a coleta de endereços de e-mail, aplicativos instalados, números de série e demais informações de identificação pessoal que se possa utilizar para rastrear usuários. Estes aplicativos representaram uma invasão da privacidade dos usuários que os baixaram, estimados em um milhão.

Ainda que há alguns anos a problemática dos códigos maliciosos afetasse predominantemente os computadores, atualmente também representa um risco para os usuários de smartphones.

Por último, não se deve esquecer do **YiSpecter**, um código malicioso para iOS que se aproveita de API privado no sistema operacional para implementar funcionalidades maliciosas. O alarmante do caso é que ele afeta dispositivos iPhone que tenham feito o jailbreak ou não. Este malware pode baixar, instalar e colocar em funcionamento aplicativos para iOS arbitrários, incluindo aqueles que substituem os verdadeiros já instalados no dispositivo.

Outros riscos no uso de smartphones

Outros riscos no uso de smartphones

Spam

O envio massivo de lixo eletrônico por parte de terceiros agora se soma a outros canais de comunicação próprios dos telefones móveis, como as mensagens de texto (SMS) e multimídia (MMS) com a finalidade de distribuir publicidade ou, em alguns casos, propagar códigos maliciosos.

Ainda que o spam não necessariamente resulte perigoso para a integridade da informação, estatísticas indicam que aproximadamente a metade dos casos estão relacionados a fraude e os demais representam uma perturbação ou distração para o usuário.

Roubo ou extravio físico do dispositivo

Neste tipo de situação, o maior problema não é a perda do dispositivo em si e o prejuízo econômico que o acompanha, mas sim a impossibilidade de recuperar a informação não respaldada e o mau uso que se possa fazer dela. Por isso, é necessário que o usuário entre em contato de imediato com a empresa prestadora de serviços de telefonia móvel que tenha contratado, como também que conte com um software que permita a remoção de informação de forma remota. Ambas ações poderão ser de grande ajuda para proteger a privacidade e confidencialidade da informação.

Roubos multiplataforma

Há muito tempo, é possível observar um aumento na quantidade e complexidade de campanhas de fraudes difundidas através de aplicativos móveis para redes sociais e mensagens instantâneas, como Facebook e WhatsApp. Algumas delas **afetaram marcas de diversas lojas muito populares** – Zara, Starbucks e McDonald's, entre outras – roubando dados pessoais das vítimas.

A Engenharia Social é um dos pontos fortes neste tipo de fraude, o que novamente evidencia porque a educação é a primeira barreira de proteção; nesse sentido, é necessário refletir e alertar sobre estas novas tendências que aplicam técnicas antigas a novos canais de comunicação.

Phishing

Técnica que consiste em obter informação pessoal ou financeira do usuário, fazendo-o acreditar que quem solicita esses dados seja alguém de confiança, como um banco ou uma empresa reconhecida. Geralmente, o phishing chega como um e-mail no qual se assusta a vitima com ameaças falsas para que digite certas informações sensíveis e privadas. No mundo móvel, esta ameaça também pode se propagar por mensagem de texto ou chamadas telefônicas.

Exploração de vulnerabilidades

Os erros de código na programação de um software são conhecidos como vulnerabilidades. Através delas, os cibercriminosos podem infiltrar-se para comprometer um sistema e roubar informação. Isso é conhecido como exploração de vulnerabilidades, algo que se tornou um mecanismo cada vez mais vigente entre os hackers para ganhar o controle dos dispositivos.

Isso representa uma nova pressão para a rápida atualização e implementação de patches nas plataformas, o que pode causar uma importante falha para sistemas operacionais como o Android, pois existe tamanha quantidade de provedores de equipamentos que as atualizações podem tardar demasiadamente em ser desdobradas aos usuários finais.

Particularmente no Android, o **Stagefright** foi uma das falhas mais conhecidas, que alarmou a mais de 950 milhões de usuários potencialmente afetados, ao permitir o roubo de informação através de código executado de maneira remota, somente enviando um SMS preparado para tal fim. Mas também é possível recordar falhas em aplicativos, como a importante **falha de segurança no SwiftKey, o aplicativo de teclado da Samsung**.

Por sua parte, o iOS também se viu comprometido através de numerosas falhas. Em meados de 2015, um **artigo acadêmico** revelou uma série de falhas que, combinadas, poderiam explorar apps maliciosos para obter acesso não-autorizado aos dados armazenados por outros aplicativos (senhas de iCloud, tokens de autenticação ou credenciais web armazenadas no Google Chrome). Além disso, outra vulnerabilidade no **Airdrop do iOS** permitu instalar apps maliciosos aparentemente legítimos com grande sigilo.

A importância de configurar e utilizar corretamente os serviços e aplicativos

A importância de configurar e utilizar corretamente os serviços e aplicativos

Compras e pagamentos de serviços a partir de um smartphone

Os smartphones e tablets, igual aos computadores, podem ser utilizados para comprar produtos, contratar serviços e realizar transações bancárias online. Ainda que estas características indubitavelmente facilitem a vida cotidiana das pessoas, também podem transformar-se em um problema grave se não se adotam as medidas de segurança necessárias. Neste sentido, já foram reportados vários casos de códigos maliciosos móveis que roubam informação sensível deste tipo.

Por isso, é vital utilizar somente aplicativos reconhecidos, baixados a partir do site oficial do fabricante e que os utilizem em um dispositivo protegido contra códigos maliciosos, para minimizar a probabilidade de ataques ou incidentes.

Redes Wi-Fi e Bluetooth

As tecnologias de conexão Wi-Fi permitem que o usuário possa conectar-se na internet a partir de quase qualquer lugar, como também compartilhar arquivos com outras pessoas. O que à primeira vista pode parecer algo muito útil, também pode resultar bastante peirgoso em caso de não se adotar as medidas de segurança pertinentes.

Sempre se deve evitar utilizar conexões Wi-Fi públicas sem proteção ou chave. Caso não seja possível, a recomendação é não realizar transações bancárias e nem utilizar serviços que requeiram informação sensível por esse meio. Além disso, o Bluetooth deve permanecer desligado se não estiver sendo ut parlizado para evitar a propagação de worms e o desgaste desnecessário de bateria.

Redes Sociais

As redes socials permitem um nível de interação impensado antes de sua invenção. Além disso, elas conseguiram um grande impacto e alcance em pouco tempo. Desta forma, suas características fazem com que estes serviços sejam muito atrativos para os usuários. Entretanto, o mesmo ocorreu com os cibercriminosos que investem tempo e recursos criando códigos maliciosos que se propagam por estas vias. Por outro lado, uma configuração incorreta da conta da rede social pode expor informação do usuário a terceiros, facilitando o roubo e a suplantação de identidade.

É recomendável analisar a configuração que as redes sociais oferecem nestes dispositivos e, se a segurança não for ótima, evite utilizá-las em redes Wi-Fi públicas onde a privacidade dos dados não é garantida.

É vital utilizar somente aplicativos reconhecidos, baixados a partir do site oficial do fabricante

Boas práticas e recomendações

1 Implementar uma solução de segurança integral

Ela deve detectar malware proativamente, filtrar mensagens não solicitadas, revisar a configuração do telefone e oferecer a possibilidade de apagar remotamente toda a informação armazenada em caso de roubo ou extravio.

2 Instalar aplicativos provenientes de repositórios ou lojas oficiais

Utilizar software legítimo proveniente de fontes e repositórios oficiais ajuda a minimizar a possibilidade de tornar-se uma vítima de códigos maliciosos. Mesmo assim, é importante que as permissões que um app demanda tenham coerência com o que ele diz fazer, bem como a avaliação da reputação do desenvolvedor.

3 Atualizar o sistema operacional e os aplicativos

Igual aos computadores, atualizar tanto o sistema operacional como os programas é necessário para obter melhorias de segurança e novas funcionalidades.

4 Estabelecer senhas de bloqueio

É recomendável que tenha mais de quatro caracteres.

5 Criptografar o dispositivo

Alguns sistemas operacionais possuem criptografia padrão, enquanto outros como o Android não. Ativar a criptografia ajudará a proteger a confidencialidade dos dados se o equipamento cair em mãos erradas.

6 Respaldar a informação

É recomendável realizar cópias de segurança periódicas da informação armazenada no dispositivo. Também se deve evitar escrever informações sensíveis como senhas em forma de lembretes ou mensagens de texto.

7 Evitar o rooting ou jailbreaking

Estes processos rompem o esquema de segurança que os sistemas operacionais são capazes de fornecer, o que facilita a instalação de ameaças.

8 Desativar opções não utilizadas como Bluetooth ou GPS

Deste modo, se evita a propagação de códigos maliciosos e o gasto desnecessário de bateria.

9 Evitar utilizar redes Wi-Fi públicas

A não ser que seja imprescindível, não usar serviços que requeiram informação sensível como transações bancárias, compras, etc.

10 Configurar adequadamente as redes sociais

Não compartilhar informação de forma pública e limitar a quantidade de amigos.

11 Não seguir hiperlinks suspeitos de e-mails, mensagens ou sites

Mesmo que estas mensagens venham de contatos conhecidos, pois eles podem estar infectados. Tampouco escanear qualquer código QR.

12 Ser cuidadoso com o dispositivo para evitar seu roubo ou perda

Não deixar o smartphone sem supervisão. É recomendável utilizar a funcionalidade mãos livres em lugares com muitas pessoas.

13 Treinar-se para detectar infecções a tempo

Recorrer a um profissional em caso de notar comportamentos estranhos do sistema ou aplicativos, o histórico de chamadas ou mensagens contiver entradas desconhecidas, existir um excessivo uso de dados, se receber mensagens estranhas de SMS, se a fatura de gastos tiver movimentos suspeitos ou qualquer outro indício similar.

Conclusão

As estatísticas demonstram que o malware móvel se diversifica a uma taxa constante, materializando-se como um vetor de ataque real. O ponto de inflexão para a proteção reside na compreensão e assimilação desta problemática, para logo se avaliar corretamente todos os riscos aos quais se está exposto e as barreiras de proteção disponíveis para neutralizá-los.

Atualmente, os cibercriminosos concentram grande parte de seus recursos na criação de ameaças para este mercado que cresce a passos largos. Por este motivo, se o uso dado aos dispositivos móveis for incorreto e não houver concientização acerca das ameaças que existem e nem se forem adotadas as medidas necessárias para resguardar a informação, qualquer usuário poderá se tornar uma nova vítima.

Neste contexto, é fundamental tomar consciência da informação que se transporta e utiliza nestes tipos de dispositivos e colocar em prática medidas de precaução para resguardá-la a fim de não sofrer nenhum incidente que possa ocasionar consequências indesejáveis.

www.eset.com.br

/esetbrasil @eset_brasil /company/eset-brasil