Saiba como se proteger da falha no protocolo de segurança do Wi-Fi [1]

O mundo da tecnologia foi pego de surpresa nesta segunda-feira, 16, com a notícia de que o protocolo WPA2, utilizado por basicamente todos os roteadores modernos para proteger redes sem fio, é vulnerável a um ataque batizado de KRACK. A sigla, que significa "ataque de reinstalação de chaves" atinge praticamente todos os dispositivos conhecidos que usam Wi-Fi.

O **Olhar Digital** preparou um guia para entender a ameaça e permitir saber como se proteger. Confira a seguir:

O que é o KRACK?

O KRACK é uma vulnerabilidade no protocolo WPA2 usado em redes Wi-Fi pelo mundo todo descoberta pelo pesquisador Mathy Vanhoef. A brecha não está nos produtos que usam o Wi-Fi e sim no padrão de redes sem fio por si só, então praticamente tudo que está conectado na internet sem usar cabos está vulnerável.

Como funciona o ataque?

Para as redes Wi-Fi funcionarem, é preciso que dispositivo e roteadores se comuniquem. Essa comunicação começa com algo chamado de "handshake", que, em bom português, se traduz como "aperto de mão". O recurso é, de forma resumida, uma série de ações que acontecem em segundo plano para que os aparelhos se reconheçam e comecem a funcionar em conjunto.

Neste caso específico, o handshake possui quatro etapas. É na terceira dessas etapas que a vulnerabilidade reside, se o hacker conseguir reinstalar uma chave já em uso (daí o nome do ataque traduzido acima). Cada chave deve ser única e nunca mais deve ser reutilizada. No entanto, a brecha do WPA2 permite refazer esse handshake manipulando a chave para que seja reutilizada, permitindo a interceptação da rede Wi-Fi.

Meu computador/celular/tablet é vulnerável?

Sim, não importa muito qual é a marca do seu dispositivo, ou qual sistema operacional ele usa. Se ele usa Wi-Fi, ele provavelmente usa o protocolo WPA2 e está na lista dos aparelhos vulneráveis.

Todos os aparelhos são igualmente vulneráveis?

Não. Existem níveis diferentes de vulnerabilidade, e as informações até agora apontam que os celulares Android estão no topo da lista dos mais vulneráveis; curiosamente, os pesquisadores também notaram que as versões mais recentes (a partir de 6.0) estão expostas do que as antigas.

---

[1] Renato Santino 16/10/2017 15h10 cibercrime Crackers Crimes digitais

Isso não quer dizer que o seu aparelho não-Android esteja livre de riscos. iOS, macOS, Windows e Linux também estão na lista de vulneráveis. Apenas estão abaixo do Android na escala de insegurança.

Qual o risco que eu corro com essa brecha?

É pelas redes Wi-Fi que circulam algumas de nossas informações mais delicadas. Fotos, mensagens, informações bancárias, senhas... tudo o que estiver trafegando sem criptografia pode ser interceptado por alguém que use essa brecha com más intenções.

A Equipe de Prontidão para Emergências Computacionais dos EUA (US-CERT) emitiu um alerta, como nota o site Ars Technica, apontando que essa brecha também permite outros tipos de ataque que vão além da interceptação direta das informações. Entre elas estão o "sequestro" de conexões TCP e injeção de conteúdo HTTP, o que significa que o hacker pode incluir código malicioso em algum site, mesmo se ele estiver seguro. Ou seja: só de entrar em algum site cotidiano você pode ter seu PC infectado com algum vírus grave como um ransomware, que bloqueia o uso do seu aparelho e o acesso aos seus arquivos e só libera mediante pagamento de resgate.

Existem casos registrados de hackers usando essa brecha?

Vanhoef, o pesquisador que revelou a falha, não sabe dizer se a vulnerabilidade já foi ou está sendo utilizada para a realização de ataques no mundo real. A posição do US-CERT parece ser a mesma.

Qual é a chance de eu ser atacado com essa brecha?

Felizmente, a chance é baixa. Para que esse ataque tenha sucesso, você e o hacker precisam estar conectados na mesma rede Wi-Fi, segundo Alex Hudson, diretor de tecnologia do Iron Group. Ou seja: é pouco provável que você esteja em risco em casa, mas fique muito atento às redes públicas.

Como me protejo?

O método mais eficaz é não se conectar a redes Wi-Fi. Pronto, você está invulnerável, principalmente as redes abertas e públicas, pelo menos até que o problema seja sanado.

Não dá para fazer nada sem Wi-Fi.

É, infelizmente a solução acima não funciona para muita gente. Neste caso, é recomendável esperar atualizações de segurança vindas do fabricante dos seus dispositivos e tomar cuidado enquanto isso não acontece. A Microsoft, por exemplo, já liberou uma correção para o Windows e é recomendável baixá-la o quanto antes. O Google prometeu uma correção para breve. A Apple deve fazer o mesmo, assim como as distribuidoras do Linux. Fique de olho e atualize seus dispositivos.

Enquanto seu aparelho não está atualizado, vale a pena evitar redes Wi-Fi públicas. O conselho valia antes do KRACK e agora só é reforçado. Serviços de VPN também são uma medida de segurança bem-vinda para trafegar de modo mais seguro em redes Wi-Fi públicas, já que o tráfego é criptografado, tornando a vida de um hacker conectado à mesma rede que você muito mais difícil.

Trocar a senha do meu roteador ajuda?

Não muito. O problema não está na senha do seu roteador, e sim no protocolo usado por ele e a proteção que ele oferece às informações que trafegam pela sua rede. A troca da senha não traz benefício prático de segurança; a única vantagem teórica é que a mudança pode expulsar da rede alguém que tenha se conectado com más intenções.

É mais eficiente verificar se há alguma atualização de segurança pendente para o seu roteador. A tendência é que neste momento ainda não esteja disponível nada criado especificamente para impedir o KRACK, mas é uma boa prática de segurança verificar regularmente se há ou não updates para o seu roteador.