Q-Day: entenda a ameaça quântica que pode quebrar a internet

Category: GERAL,TECNOLOGIA e CIÊNCIA
escrito por Maria Luiza | 18 de maio de 2026

O relógio conta regressivamente para o Q-Day, a data iminente – ainda desconhecida – em que a computação quântica terá capacidade de quebrar de forma rápida e fácil as chaves de criptografia que mantêm a maior parte das comunicações na internet seguras.

Especialistas conhecem o risco hipotético do Q-Day desde a década de 1990. Mas o Google alertou recentemente que computadores quânticos podem ser capazes de hackear alguns sistemas criptografados até 2029 – um prazo que reduz drasticamente a janela para proteger dados, em comparação com o que muitos especialistas em cibersegurança haviam previsto anteriormente. A nova estimativa significa que governos, empresas e outras entidades podem ter muito menos tempo para se preparar.

“É o dia em que pessoas, talvez adversários, terão acesso a um computador quântico capaz de quebrar códigos criptográficos que estão em uso”, disse Michele Mosca, cofundador e CEO da empresa de cibersegurança evolutionQ.

O Q-Day marca o momento em que um computador quântico adquire recursos e estabilidade suficientes para decifrar a criptografia convencional. Quando isso acontecer, cada

transação financeira, arquivo médico, e-mail, histórico de localização e carteira de criptomoedas protegidos pelos algoritmos comumente usados hoje poderiam ser desbloqueados por uma máquina capaz de resolver a matemática complexa que atualmente mantém os dados sensíveis seguros.

Nesse ponto de virada transformador, "tudo está seguro – seguro, seguro – e de repente não está mais seguro. É um salto muito drástico", disse Mosca, que também é professor do Institute for Quantum Computing da University of Waterloo, em Ontario.

Adversários e agentes mal-intencionados podem já estar coletando dados criptografados, com a intenção de lançar ataques do tipo "colher agora, descriptografar depois". Nesse cenário, informações são roubadas, armazenadas e depois descriptografadas quando um computador quântico em escala completa estiver disponível, acrescentou ele.

Mosca é coautor do Quantum Threat Timeline Report, publicado pelo Global Risk Institute em Toronto, desde 2019. A sétima edição, publicada em 9 de março, sugeriu que um computador quântico em escala completa e criptograficamente relevante era "bastante possível" nos próximos 10 anos, e "provável" nos próximos 15. Mosca e seu coautor basearam sua previsão nas opiniões de 26 especialistas.

"Muitas organizações podem não ter consciência de que estão atualmente expostas a um nível intolerável de risco que exige ação urgente", escreveram os autores do relatório.

O Google afirmou, em 25 de março, que tinha como meta o ano de 2029 "para garantir a segurança da era quântica" com criptografia pós-quântica. A empresa disse que o prazo refletia os avanços no campo da computação quântica. "Ao fazer isso, esperamos fornecer a clareza e a urgência necessárias para acelerar as transições digitais não apenas para o Google, mas também em todo o setor", observou em uma publicação em seu

blog. De forma semelhante, a empresa de serviços de computação em nuvem CloudFlare anunciou que também passou a ter como meta o ano de 2029. O Google recusou um pedido de entrevista.

A canalização invisível

A criptografia é a canalização invisível que mantém a economia global em funcionamento. A maior parte da segurança na internet – pense no símbolo do pequeno cadeado no seu navegador – é atualmente baseada em criptografia que depende de uma peculiaridade matemática. Embora multiplicar números seja relativamente fácil, o processo inverso – a fatoração – não é.

A criptografia RSA – batizada com as iniciais de seus criadores Ron Rivest, Adi Shamir e Leonard Adleman – é um dos algoritmos de criptografia mais comuns e utiliza essa abordagem. O Quantum Threat Timeline Report define um computador criptograficamente relevante como aquele que poderia, por exemplo, quebrar a criptografia RSA em 24 horas.

A computação quântica não é simplesmente uma versão mais poderosa ou mais rápida dos computadores em uso hoje. Essa forma de processamento funciona de maneira fundamentalmente diferente.

Ao contrário dos computadores convencionais, que processam informações sequencialmente usando bits (0 ou 1), os computadores quânticos empregam bits quânticos – "qubits" – que podem representar 0, 1 ou ambos simultaneamente. Conhecida como superposição, essa propriedade permite que as máquinas quânticas armazenem e processem informações mais complexas.

O principal desafio que o campo precisa superar é tornar os qubits físicos mais estáveis. Esses componentes sensíveis geralmente funcionam apenas em ambientes extremamente frios e de alto vácuo – condições que ajudam a mantê-los estáveis e menos sujeitos a erros durante os cálculos.

“Tiro de advertência”

Futuros computadores quânticos podem ser capazes de quebrar a criptografia de segunda geração que protege criptomoedas e outros sistemas com muito menos qubits do que se imaginava anteriormente, de acordo com um relatório de março. O artigo foi coassinado por funcionários do Google e acadêmicos da University of California Berkeley, da Stanford University e da Ethereum Foundation, uma organização sem fins lucrativos que apoia o blockchain Ethereum.

Conhecida como criptografia de curva elíptica, ou ECC, a técnica de criptografia utiliza uma matemática mais obscura do que o algoritmo RSA; ela se baseia em equações que podem ser representadas como linhas curvas em um gráfico e gera chaves de criptografia com base em diferentes pontos da linha.

O Google afirmou, em uma publicação de blog datada de 31 de março, que a equipe de pesquisa encontrou uma redução de aproximadamente 20 vezes no número de qubits físicos necessários para resolver o problema matemático fundamental que sustenta a ECC. A empresa acrescentou que desenvolveu um novo método para descrever as vulnerabilidades de segurança que os futuros computadores quânticos representam, “para que possam ser verificadas sem fornecer um roteiro para agentes mal-intencionados”.

A maioria das tecnologias blockchain e das criptomoedas depende atualmente da criptografia de curva elíptica para aspectos críticos de sua segurança, disse a publicação do Google. Embora existam soluções viáveis, a publicação acrescentou que “elas levarão tempo para ser implementadas, aumentando a urgência de agir”.

O artigo ainda não foi revisado por pares, mas pode ser considerado um “tiro de advertência”, especialmente para a comunidade de criptomoedas, disse Catherine Mulligan, acadêmica visitante e pesquisadora associada do Institute for

Security Science and Technology do Imperial College London.

“As criptomoedas são inerentemente incrivelmente descentralizadas”, ela disse. “O problema é que, para fazer uma atualização, é preciso obter a concordância das pessoas, é preciso alcançar consenso entre os próprios engenheiros para realizar a atualização, e eles tendem a discutir muito sobre como farão essa atualização”, disse Mulligan.

A boa notícia, ela explicou, é que governos, incluindo os dos Estados Unidos e do Reino Unido, publicaram padrões para a criptografia pós-quântica.

Essas diretrizes envolvem principalmente atualizações de software que dependem de uma matemática “ordens de magnitude mais complexa” para ser resolvida do que as abordagens tradicionais, disse Mulligan. Além disso, algumas empresas e governos podem combinar isso com a criptografia quântica de chaves, especialmente para informações altamente sensíveis.

A criptografia quântica de chaves permite que duas partes que desejam compartilhar dados sensíveis estabeleçam uma chave de criptografia segura, com o sigilo garantido pelas leis da física, e não pela dificuldade computacional de um problema matemático.

O protocolo, concebido pela primeira vez na década de 1980 pelos vencedores do Prêmio Turing deste ano, envolve o uso de fótons de luz para criar uma chave secreta entre duas partes. No entanto, o método requer hardware especializado, o que pode torná-lo mais caro e difícil de implementar.

Alguns pesquisadores comparam a ameaça quântica ao Y2K, ou bug do milênio, uma falha de computador que os programadores acreditavam poder causar graves problemas sistêmicos após 31 de dezembro de 1999.

Quando os primeiros programas de computador estavam sendo escritos, os engenheiros usavam um código de dois dígitos para

o ano, pois naquela época o armazenamento de dados era caro. Por exemplo, para o ano de 1977, a data era registrada como 77. À medida que o ano 2000 se aproximava, os programadores perceberam que os computadores poderiam não interpretar 00 como 2000, mas como 1900, potencialmente causando transtornos.

“Eu sei que temos esses cenários apocalípticos, nos quais estamos assustando todo mundo”, disse Mulligan. “Sou velha o suficiente para me lembrar do Y2K. Basicamente, a razão pela qual o Y2K não aconteceu é que todos trabalharam arduamente o suficiente para garantir que não acontecesse.” Mulligan disse acreditar que provavelmente seria isso o que aconteceria com a ameaça quântica à cibersegurança.

No entanto, não está claro se a nova ameaça será enfrentada com urgência semelhante. Pouco mais de 90% das empresas ainda não têm um roteiro para lidar com ameaças de segurança quântica, de acordo com dados citados pela McKinsey.

Os custos potenciais de uma preparação inadequada são assombrosos.

Um relatório de 2023 do Hudson Institute, um think tank conservador dos EUA, estimou que um ataque cibernético por computador quântico ao Fedwire Funds Service do Federal Reserve – seu sistema de pagamentos interbancários – poderia desencadear um colapso financeiro e resultar em uma recessão econômica de seis meses.

Dustin Moody, um matemático envolvido em criptografia pós-quântica no National Institute of Standards and Technology, agência federal dos Estados Unidos, disse que grandes empresas multinacionais estavam bem cientes da ameaça e “avançando com bastante rapidez”. No entanto, ele afirmou que havia um limite para as ações que indivíduos e pequenas empresas poderiam tomar.

“Todos deveriam estar preocupados e apreensivos com isso”,

disse Moody. “O que a pessoa comum precisa fazer? Nada. Quer dizer, ela precisa confiar em seus provedores de tecnologia e afins para lidar com essa mudança por ela”, disse ele.

“Da mesma forma com empresas menores e familiares, elas próprias não precisam fazer muito, desde que garantam que os produtos que estão usando – que conversem com os fornecedores e digam: ‘Existe essa ameaça quântica, vocês já cuidaram disso?'”, acrescentou.

A Casa Branca recomenda 2035 como o ano em que as entidades deveriam ter adotado a criptografia pós-quântica, disse Moody. O NIST finalizou um conjunto de algoritmos de criptografia em 2024, projetados para resistir a ataques cibernéticos de um computador quântico.

“Se todos migrassem a tempo, estaríamos em boa situação, mas o problema é que isso não vai acontecer no mundo real”, disse ele. “Já tivemos migrações criptográficas no passado, passando de um algoritmo para outro – tipicamente isso leva de 10 a 20 anos – e essa migração será mais complicada e mais custosa do que as anteriores. Portanto, se um computador quântico surgir em cinco anos, a transição ainda não estará concluída”.

Além disso, enquanto as organizações adotam proteção segura contra ameaças quânticas, fazer isso apenas defenderá dados futuros contra a ameaça quântica, observaram Moody e Mulligan, dado o risco de que ataques do tipo “armazenar agora, descriptografar depois” possam já estar em andamento.

Registros eletrônicos de saúde, que contêm históricos médicos de longo prazo e informações genéticas, poderiam ser alvos prioritários para esses tipos de ataques. “O fato é que você pode atualizar seu software, mas não pode realmente atualizar seu DNA”, disse Mulligan.

Dispositivos biomédicos em risco

Seoyoon Jang, doutoranda em engenharia elétrica e ciência da computação no Massachusetts Institute of Technology, trabalha

para proteger dispositivos biomédicos sem fio, como bombas de insulina e marcapassos, de possíveis ataques quânticos. Esses dispositivos minúsculos e amplamente utilizados geralmente têm restrições de energia demais para executar os protocolos de segurança computacionalmente exigentes necessários em um mundo pós-quântico.

Ela descreve um cenário de pior caso no qual o dispositivo externo – frequentemente um smartphone que se conecta sem fio à bomba de insulina para regular a dosagem – é hackeado. “Imagine como seria fácil enviar um comando: “Ei, libere uma dosagem letal.” Temos que realmente nos preocupar com isso”, disse ela. “À medida que avançamos para o monitoramento remoto de saúde, esses dispositivos estarão em todo lugar”.

Junto com seus colegas, Jang desenvolveu um microchip ultraeficiente, com tamanho aproximado ao de uma ponta de agulha extremamente fina, que inclui proteção integrada necessária para a cibersegurança pós-quântica. O dispositivo alcançou entre 20 e 60 vezes maior eficiência energética do que outras técnicas de segurança pós-quântica com as quais foi comparado. O microchip tem uma área menor do que muitos chips existentes.

O trabalho foi parcialmente financiado pela Advanced Research Projects Agency for Health, ou ARPA-H, que, segundo Jang, planejava comercializar a tecnologia. “Meu chip é, até onde eu sei, o primeiro a realmente tentar preencher essa lacuna”, disse ela. A ARPA-H faz parte do Departamento de Saúde e Serviços Humanos dos EUA.

O mais recente Quantum Threat Timeline Report afirmou que é particularmente difícil avaliar o risco quântico à cibersegurança porque esforços de pesquisa “sob o radar” – por laboratórios secretos apoiados por estados, empresas operando em sigilo ou atores privados mal-intencionados – podem significar que os avanços na computação quântica estão ocultos.

“Como sucessos encobertos permaneceriam invisíveis por algum tempo, é mais seguro presumir que a verdadeira ameaça pode estar mais próxima do que se pode inferir apenas a partir de publicações abertas”, disse o relatório. “O verdadeiro Q-day pode ocorrer antes que o mundo tome conhecimento dele, já que estados ou atores mal-intencionados potencialmente buscam usar esse conhecimento em seu benefício estratégico”.

Fonte: cnnbrasil e Publicado Por: Jornal Folha do Progresso 18/05/2026/06:23:11

O formato de distribuição de notícias do Jornal Folha do Progresso pelo celular mudou. A partir de agora, as notícias chegarão diretamente pelo formato Comunidades, ou pelo canal uma das inovações lançadas pelo WhatsApp. Não é preciso ser assinante para receber o serviço. Assim, o internauta pode ter, na palma da mão, matérias verificadas e com credibilidade. Para passar a receber as notícias do Jornal Folha do Progresso, clique nos links abaixo siga nossas redes sociais:

- **Clique aqui e nos siga no X**
- **Clica aqui e siga nosso Instagram**
- **Clique aqui e siga nossa página no Facebook**
- **Clique aqui e acesse o nosso canal no WhatsApp**
- **Clique aqui e acesse a comunidade do Jornal Folha do Progresso**

Apenas os administradores do grupo poderão mandar mensagens e saber quem são os integrantes da comunidade. Dessa forma, evitamos qualquer tipo de interação indevida. Sugestão de pauta enviar no e-mail:folhadoprogresso.jornal@gmail.com.

Envie vídeos, fotos e sugestões de pauta para a redação do JFP (JORNAL FOLHA DO PROGRESSO) Telefones: WhatsApp (93) 98404

6835– (93) 98117 7649.

“Informação publicada é informação pública. Porém, para chegar até você, um grupo de pessoas trabalhou para isso. Seja ético. Copiou? Informe a fonte.”

Publicado por Jornal Folha do Progresso, Fone para contato 93 981177649 (Tim) WhatsApp:-93- 984046835 (Claro) -Site: www.folhadoprogresso.com.br e-mail:folhadoprogresso.jornal@gmail.com/ou e-mail: adeciopiran.blog@gmail.com

Lignosulfonato de sódio no Brasil: onde e por que ele é utilizado