Brasil é um dos principais alvos de ataques à segurança

De São Paulo

O nível de ameaças baseadas em IoT se mantém elevado. A especialista em cibersegurança Kaspersky registrou 105 milhões de ataques contra dispositivos IoT no primeiro semestre, vindos de 276 mil endereços exclusivos IP. O levantamento foi feito com ajuda de uma rede de dispositivos conectados (honeypots) usada como isca para investigar as atividades criminosas.

O Brasil foi alvo de 19% dos ataques, só perdendo para a China. A família Mirai, que há dois anos derrubou serviços como Twitter e Amazon, está por trás de 39% dos ataques maciços de negação de serviço (DDoS) ou retransmissão de campanhas maliciosas, como as de mineração de criptomoedas ou phishing.

A massificação é uma das características dos ataques relacionados a dispositivos de IoT, com baixo poder de processamento e sem soluções de segurança, como antivírus. Mas, mesmo em dispositivos com mais recursos, a segurança é uma das últimas configurações a atrair usuários domésticos. Isso vale desde a mudança de senhas padrão de roteadores até configurações mais sofisticadas de assistentes pessoais. "Continuamos vendo ataques massivos com fins financeiros, como coleta de credenciais. São mais de 2,5 bilhões de credenciais expostas e o número aumenta até o fim do ano com as datas comerciais", diz Thiago Bordini, diretor de inteligência cibernética da New Space. "A segurança está na mão dos usuários."

Pesquisa realizada pela Eset no ano passado mostrou que 70% deles acreditam que dispositivos IoT são inseguros, mas 62% se mostravam dispostos a adquiri-los. Troca de senha padrão, habilitação de configurações de segurança e atualização de software ou, se for o caso, de equipamento, são passos primários para o segmento. Mas ele também é refém da preocupação por parte de operadoras e empresas que desenvolvem aplicativos e dispositivos, lembra o pesquisador de segurança da Eset, Daniel Barbosa.

A Cyxterra também conduziu com a Universidade de Tecnologia e Design de Cingapura experimento com honeypot com 44 dispositivos de IoT expostos e em um ano identificou mais de 150 milhões de requerimentos de conexão não solicitados. Também apontou que mais de 90% das transações de dados em dispositivos IoT não são criptografadas. Para empresas que adotam IoT, a marca propõe estratégia baseada na redução da superfície de ataque, com avaliação de ativos tecnológicos expostos, garantia de acesso seguro, com autenticação e verificação de identidade, e neutralização para mitigar prejuízos, diz o vice-presidente para a América Latina da Cyxterra, David López.

"A maturidade de segurança dos ativos tradicionais de TI está em nível muito mais alto do que dos ativos de IoT", aponta o sócio de cibersegurança da EY, Marcos Sêmola. Além de encapsulamento de processos críticos operados pelos dispositivos IoT, ele defende a segurança como parte de um projeto anterior à entrada em linha de produção (security by design).

Com a tecnologia apoiando a expansão das ameaças — a varredura de vulnerabilidades, por exemplo, fica a cargo de robôs — surgem iniciativas institucionais e regulamentação envolvendo IoT, inclusive no Brasil.

A certificação de dispositivos foi um dos temas da recente consulta pública da Anatel sobre IoT. Em discussão estão questões como qual o nível de proteção em caso de armazenamento de dados nos dispositivos, necessidade de criptografia para transmissão, autenticação de usuários e controle de acesso, aponta Emilio Nakamura, especialista em segurança do CPqD.

Também entram em pauta questões relacionadas a desenvolvimento seguro, como validação dos dados de entrada, para evitar execução de comando que dê acesso administrativo ao dispositivo, e limpeza adequada de memória, impedindo alocação indevida que permita execução de código malicioso. *(MF)*