

Empresa do Reino Unido lança tecnologia que bloqueia ataques ransomware

Solução age de forma imediata para prevenir e interromper ataques do dia zero, detectar variações de exploits, ameaças desconhecidas e ataques ransomware

22/09/2016 15:24:38

A Sophos, líder global em segurança de rede e endpoint, anuncia o lançamento do Sophos Intercept X, uma solução de segurança endpoint que interrompe ataques do dia zero, detecta variações de exploits e ameaças desconhecidas, além de agregar recurso anti-ransomware que previamente protege contra este tipo de ataque.

O Sophos Intercept X reúne em um única solução quatro componentes de segurança crítica para proteção, que oferece rápida identificação e resposta para as ameaças e, também, elimina a necessidade de equipe especializada na sua implementação e uso. São eles:

1. Ameaça Signatureless ou Detecção de Exploit: anti-malware e anti-hacker, bloqueia o ataque do dia zero desconhecido e de memória residente, além de variações de ameaças sem a necessidade de escaneamento de arquivos.
2. CryptoGuard: anti-ransomware, identifica e interrompe atividade maliciosa de criptografia, boqueando o ransomware antes que ele possa restringir o acesso ao sistema infectado, criptografar e danificar os arquivos.
3. Documento de Análise de Causa de Raiz: uma visão analítica 360 graus de ameaças que mostra de onde vem os ataques, o que está impactado, onde está parado e recomenda ações de prevenção para evitar um ataque futuro.
4. Sophos Clean: poderoso serviço que busca e remove qualquer vestígio de spyware, mesmo malware profundamente enraizado e persistente.

“O uso do big data aliado ao nosso conhecimento dos padrões de ameaças, vetores de ataque e motivação criminosa, possibilitou a criação do Intercept X que reconhece comportamentos maliciosos e impede ataques potenciais antes de entrar na Kill Chain, ou seja, antes que o ataque se concretize, sem a necessidade de assinatura e atualização”, afirma Dan Sciappa, sênior vice-

presidente do Grupo de Proteção de Endpoint da Sophos.

O Intercept X é parte da estratégia de entrega de soluções de Segurança Sincronizada da Sophos e pode ser controlado remotamente por meio do Sophos Central, um console de gerenciamento baseado na nuvem que permite aos administradores configurar regras, distribuir licenças, adicionar endpoints e acompanhar todas as atividades, para uma resposta coordenada e automatizada aos ataques.

“De acordo com uma pesquisa do Grupo de Segurança de Endpoint da Sophos, muitas organizações estão adotando novas tecnologias de prevenção, mas, muitas vezes, não têm equipes com nível adequado de competências para realizar análises e executar tarefas de cybersecurity. O Intercept X dispensa profissional especializado e fornece rápida resposta de proteção, fechando lacunas de segurança no endpoint que ainda existem em todo o mundo”, afirma Tony Palmer, analista sênior do Lab da ESG.

Os clientes e parceiros que testaram a versão beta do software reconhecem a capacidade de eliminar o ransomware quase imediatamente, além de recuperar os arquivos afetados sem nenhuma alteração. "Nós instalamos a versão beta em redes de 70 clientes em mais de 2 mil endpoints. Até o momento, o software interrompeu mais de 18 novos ataques de ransomware e desde a implantação não tivemos nenhuma infecção", conta Emily Adams, analista de segurança da TI da Flexible Systems, parceira Sophos com sede em Hauppauge, Nova Iorque.

O Sophos Intercept X pode ser instalado para operar em conjunto com qualquer software de segurança endpoint existente no mercado. Bob Appleby da PA Computer Connections, empresa parceira baseada nos Estados Unidos, comentou, "Foi simples e eficaz instalar o Intercept X ao lado de proteção de endpoint existente. Ao testar o produto nós descobrimos que ele bloqueia ameaças mais rapidamente e fornece uma análise abrangente e direta de um ataque”.

Emile Belcourt da Globelink, parceira da Sophos com sede no Reino Unido disse: "Estou tendo uma experiência fácil e simples com a implementação e transição para o Intercept X. A visibilidade de ameaças irá facilitar o trabalho dos profissionais de TI para que tenham tempo disponível para fazer o que realmente importa, ao invés de se preocuparem constantemente com o monitoramento.”

James Miller, diretor da Foursys, um parceiro da Sophos com sede no Reino Unido disse: "A nossa equipe técnica testou o Intercept X e todos concordam que ele será uma segurança adicional para os nossos clientes. Com os componentes de segurança integrados em um só produto, a Sophos está simplificando o que antes era um processo complexo e difícil.”

O Sophos Intercept X está disponível globalmente e pode ser testado gratuitamente pela página da Sophos Intercept X. Para saber mais, acesse <http://www.sophos.com/> ou contate um parceiro.

