DINO - Divulgador de Notícias

Solução para endpoint previne malware conhecido e desconhecido em tempo real

Entre os recursos estão análise estática via aprendizado da própria máquina e quarentena de executáveis maliciosos

12/08/2016 13:24:55

A Palo Alto Networks, fornecedora de soluções de segurança corporativa, anuncia versão Traps 3.4, sua solução de proteção avançada de endpoint que chega ao mercado com inúmeros novos recursos: de aprendizado da própria máquina para prevenção de malware em tempo real, como exemplo, de exploits; e vem com a funcionalidade de Publisher confiável, permitindo que a solução detecte e impeça malware desconhecido de forma automática. O lançamento também reduz a necessidade de compra de antivírus a fim de proteger endpoints como notebooks, servidores e instâncias de VDI.

Muitas empresas implementam uma série de produtos e software de segurança em seus sistemas de endpoint, incluindo um ou mais antivírus tradicionais. No entanto, as violações cibernéticas continuam aumentando com frequência, variedade e sofisticação.

A solução Traps combina os métodos mais efetivos de detecção de exploit e malware para prevenir ameaças conhecidas e desconhecidas antes que possam comprometer o endpoint. Com foco em detectar e bloquear as técnicas desses ataques, o Traps pode evitar ataques sofisticados, direcionados e nunca antes vistos.

Componente da linha de segurança de próxima geração da Palo Alto Networks, uma plataforma integrada e automatizada projetada para permitir aplicações de forma segura e prevenir violações, o Traps tanto divide quanto recebe informações de inteligência de ameaças do ambiente de análise de malware baseado na nuvem, o Wildfire. A informação é enviada para o Wildfire por cada componente da plataforma e o Traps utiliza essa informação para bloquear ameaças no endpoint, não importa de onde venham.

“Os antivirus tradicionais são parte importante de um sistema de segurança da informação, mas não foram projetados para ameaças avançadas atuais. Para isso, as empresas precisam adotar uma plataforma de segurança que impeça que o malware, mesmo desconhecido, invada a empresa em qualquer ponto – incluindo o endpoint”, explica Lee Klarich, vice-presidente executivo e gerente de Produtos da Palo Alto Networks.

A versão 3.4 do Traps estará disponível no fim de Agosto no Palo Alto Networks Support Portal e inclui as seguintes atualizações:

•Análise estática via aprendizado de máquina - examina centenas de características de um arquivo para determinar se é um malware. A inteligência de ameaça disponível na assinatura do Wildfire é utilizada para treinar um modelo de aprendizado de máquina para reconhecer o malware, principalmente as variantes desconhecidas, com eficácia e precisão. Essa nova funcionalidade permite que o Traps determine rapidamente se um arquivo deve ser autorizado a executar antes de passar pelo Wildfire.

•Identificação de Publisher confiável - permite que as organizações identifiquem automaticamente em tempo real novos arquivos executáveis postados por softwares confiáveis e com boa reputação. Esses arquivos ganham permissão para serem executados, evitando análise desnecessária e permitindo a execução sem delay ou impacto para o usuário.

•Quarentena de executáveis maliciosos - remove imediatamente os arquivos maliciosos e impede tentativas de propagação ou execução dos arquivos.

•Classificação de Grayware - permite que as empresas identifiquem softwares não-maliciosos, porém indesejáveis, para impedir que sejam executados em seu ambiente.