Sistema imunológico digital promete defesa permanente contra vírus

13/09/2012 - O que tem a segurança dos computadores a ver com anticorpos, antígenos e linfócitos?

Para responder à questão, basta fazer outra pergunta: se os computadores são infectados por vírus, por que não dotá-los de um sistema imunológico?

Siga o CIÊNCIAemPAUTA no Twitter. Curta nossa página CIÊNCIAemPAUTA no Facebook!

Foi com esta analogia em mente que Isabela Liane de Oliveira, que é cientista da computação, começou a estudar imunologia, para tentar dar aos computadores o seu próprio "sistema imunológico digital".

Esta é a base de uma linha de pesquisa relativamente nova nas ciências da computação. Inspirados nos mecanismos de defesa imunológica, pesquisadores querem criar sistemas inteligentes capazes de detectar pragas cibernéticas conhecidas genericamente como malware (do inglês malicious software), que abundam na internet.

Malwares

Os malwares são programas criados geralmente para danificar a operação de um computador ou para roubar dele dados sigilosos, quase sempre com objetivo criminoso.

Dependendo da forma como agem e se replicam, os malwares podem ser classificados como vírus, cavalos de troia, worms (vermes), spywares (programas espiões) etc.

"As diferenças entre eles são pequenas, na prática podemos chamar todos de vírus", simplifica Adriano Mauro Cansian, chefe do Laboratório de Segurança de Computadores da Unesp em São José do Rio

Preto, que orientou a pesquisa de Isabela.

Enquanto os antivírus dependem de uma atualização constante, para que possam reconhecer cada novo malware que surge, a intenção dessa nova linha de pesquisas é dotar o computador de uma capacidade de detectar algo estranho e desconhecido, que possa ser inoculado tão coloca ameace fazer qualquer mal.

"Como os ataques mudam de padrão muito rapidamente, o ideal é um sistema de proteção com certo grau de adaptabilidade para acompanhar essas mudanças", explica Cansian.

Armadilha para malwares

Baseando-se em uma analogia com o sistema imunológico, o sistema desenvolvido por Isabela e Cansian visa a detecção de novos malwares em redes de computadores - as redes seriam o equivalente ao corpo.

O primeiro passo é a captura dos malwares, que pode ser feita de duas formas. Uma é a simulação de um ambiente totalmente desprotegido, que vai funcionar como armadilha. A outra depende da colaboração dos usuários, que podem permitir que um programa analisador se conecte ao servidor de e-mail e vasculhe suas mensagens pessoais.

"Esses programas não violam a privacidade dos usuários", frisa Isabela. "Apenas buscam códigos aparentemente maliciosos, que estão contidos principalmente nos anexos e nos links."

Ao encontrar suspeitos, o sistema imunológico digital fazem uma cópia deles.

Seleção negativa

Em seguida, cópias dos malwares coletados são executadas em um computador próprio para isso.

O objetivo é analisar o fluxo de dados dentro da máquina e o tráfego de rede. Um cavalo de troia, por exemplo, pode se empenhar em capturar a senha de acesso ao site do banco e enviá-la para o criador do malware, que pode estar do outro lado do mundo. Isabela ressalta que dados sigilosos, como os de acesso a contas bancárias, nunca são acessados nem armazenados pelo sistema de detecção de malwares.

Nesta etapa ocorre ainda a chamada "seleção negativa", à semelhança do que faz o sistema imunológico. No corpo humano, as células imunológicas fazem uma espécie de checagem para garantir que o suspeito é realmente um elemento estranho e não está sendo confundido com algo próprio do organismo. Isso é importante também porque alguns malwares fazem coisas como qualquer outro programa, para disfarçar sua identidade, explica Isabela.

Se ficar comprovado que o suspeito é realmente um malware, todo esse disfarce é removido, explica ela, restando apenas a parte de fato maliciosa do código. Com ela são geradas "assinaturas", que vão para um banco de dados. Elas farão o papel de receptores de células imunológicas, que têm afinidade com o elemento estranho.

Do mesmo modo que células imunológicas, como linfócitos T e macrófagos, circulam pela corrente sanguínea, o sistema desenvolvido pelos pesquisadores vigia o tráfego na rede.

E toda vez que detecta um fluxo de dados (antígeno) compatível com alguma das assinaturas armazenadas no banco de dados (receptor), automaticamente gerará um alerta para o administrador da rede, indicando-lhe as medidas que devem ser tomadas para eliminar aquele mal específico.

Camadas de segurança

Sistemas desse tipo vêm sendo desenvolvidos e testados por cientistas da computação em várias partes do mundo e ainda estão longe de se tornarem soluções comerciais. "É realmente uma pesquisa de fronteira", afirma Cansian.

Segundo ele, a ideia não é substituir outros métodos de segurança, mas agregar mais um mecanismo de defesa, que tem como diferencial a adaptabilidade. "A boa segurança deve ter várias camadas, se cair uma, tem outra."

Embora pesquisas como a de Isabela tenham seus resultados divulgados publicamente, ninguém na área gosta de falar muito dos detalhes, "por razões óbvias", segundo Cansian.

"A proteção do método faz parte da cadeia de segurança. É preciso ter esse cuidado porque a criação de malwares já é um grande negócio, uma ferramenta do crime organizado", diz.

Fonte: Inovação Tecnológica