

DNA de vírus: a busca pelo mapeamento veloz

Tempo de resposta do antivírus a ataques de pragas virtuais é realmente importante ou não passa de marketing?

Elis Montelero

Uns dizem que o assunto nada mais é que uma estratégia de marketing; outros, a diferença entre uma possível infecção e sua cura imediata. Tempo de resposta dos programas antivírus aos ataques gerados na internet é sempre uma questão polêmica, principalmente porque mexe com os bróis dos fabricantes — para um fabricante de antivírus, carregar o rótulo de “o primeiro a detectar tal ameaça” parece ser uma meta — e ainda confunde os usuários. Enfim, é verdade que quanto mais rápido o software de proteção reagir aos ataques, mais prováveis são as chances de sucesso?

Por dia, dez novos vírus ameaçam o seu micro

Como saber o tempo de resposta do antivírus? Um clique no programa pode revelar quando foi feita a última atualização. Como a média de nascimento de novos vírus, segundo as fabricantes, é de, em média, dez por dia (algumas falam em 50 por semana), dois dias sem atualizar podem significar 20 novas pragas. E ninguém quer 20 vírus rondando o micro, certo?

— Esse tempo de resposta é subjetivo porque depende da gravidade do vírus. O melhor é usar um antivírus com atualização online. Ou você atualiza na mão ou programa o antivírus para atualização periódica ou pede para o antivírus buscar atualizações o tempo todo — diz Fernando Nery, presidente da Módulo.

Correr atrás de um tempo menor na resposta aos ata-

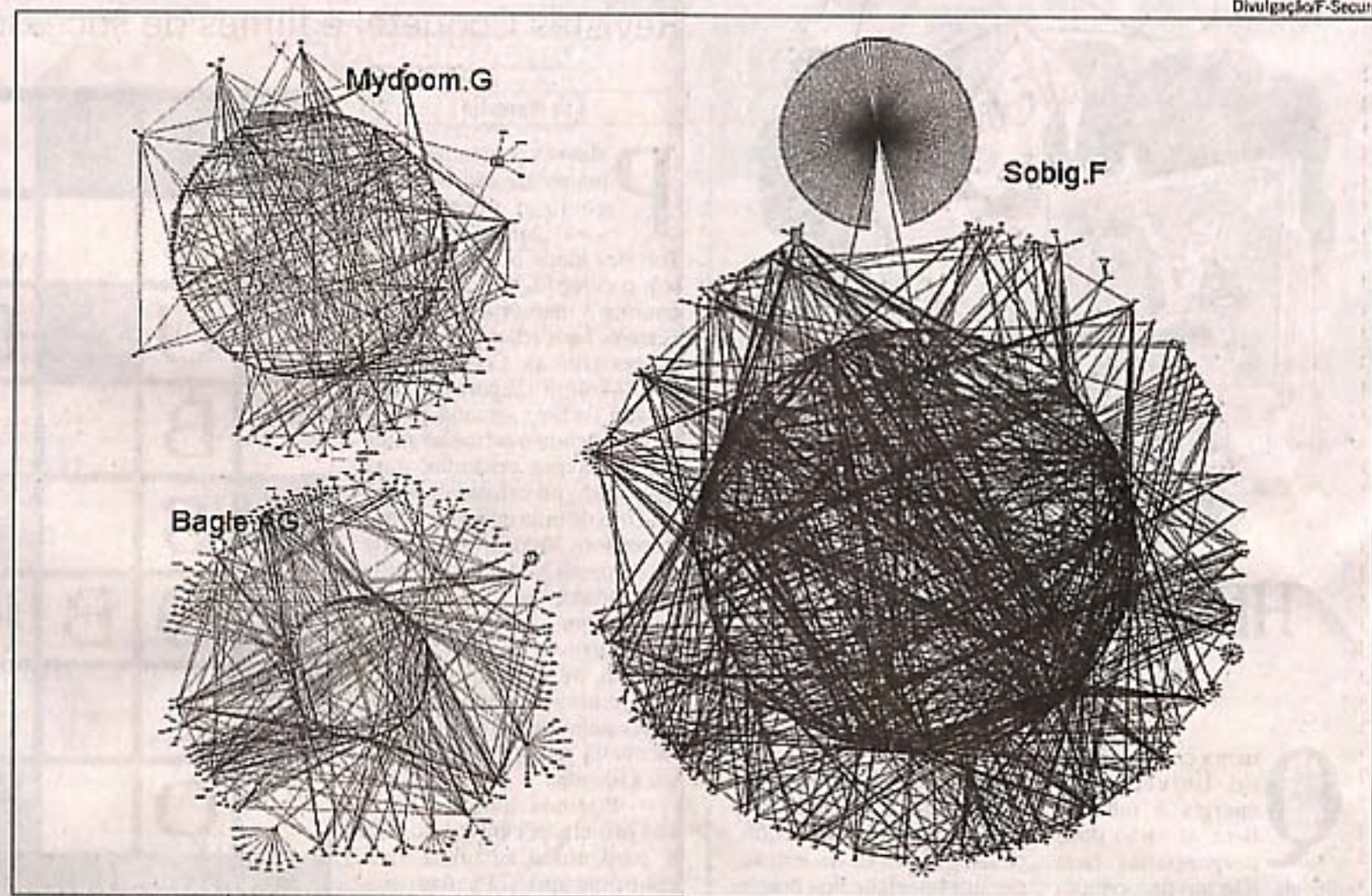
ques fez com que a empresa finlandesa F-Secure desenvolvesse um método para identificar novas pragas. Quando um código malicioso chega às mãos da fabricante, ele é mapeado e, sua imagem, guardada no banco de dados, onde terá estudado o seu DNA.

— Quando um vírus chega, verificamos sua imagem. Se ele tiver 95% de igualdade com outros códigos, ele é tratado como variante. A partir daí, é mais fácil criar a vacina. É claro que 100% de segurança é impossível, o que a gente pode fazer é trabalhar na casa dos 99,1% aos 99,9% — diz Daniel Carboni, responsável pela F-Secure no Brasil. — O DNA de um vírus computacional é tão importante quanto o de um ser humano.

Segundo a consultoria especializada em tempo de resposta Av-Test.org, a F-Secure oferece vacinas num tempo médio de seis horas. Só para se ter idéia do que isso significa: o vírus Nimda, que se alastrou em 2001, levou 360 dias para ganhar uma vacina depois que sua primeira variante foi divulgada. Há uns anos, vacinas para vírus de macros levavam de seis meses a um ano para nascerem.

“Potes de mel” para encontrar novas ameaças

Como as fabricantes de antivírus têm acesso a todo tipo de código malicioso? Usando a técnica “do urso e do mel”, literalmente. Em vários pontos do planeta, empresas, departamentos de governos e entidades civis instalam servidores “honey pots” (potes de mel), máquinas com grande capacidade de armazenamento/processamento/velocidade de banda e com



QUE COISA ESTRANHÍSSIMA é esta? Simples, ora, está na cara: é o DNA de alguns vírus bem conhecidos, em mapeamento feito pela F-Secure

pouca segurança que são infectadas “por querer”. Depois de “pegos”, os arquivos com os códigos maliciosos são enviados para laboratórios de empresas de segurança, que estudam o código e criam as vacinas.

Os fusos também precisam ser levados em consideração. Segundo pesquisas, a maior parte dos ataques parte da Ásia e do Leste da Europa — principalmente da Rússia.

— Existem incidências que certas regiões do mundo nem

percebem — diz Marc Achatz, diretor-geral da empresa de segurança Fortinet, que garante levar três horas para liberar vacinas contra vírus.

Para os críticos da indústria de antivírus, enquanto as fabricantes competem pelo menor tempo de resposta, mais rapidamente trabalham os invasores. E a indústria se alimenta deste eterno embate.

— Quanto mais vírus lançados, mais defesas são criadas. Sempre vai haver hackers

desenvolvendo novos vírus, mas alguma hora se esgotarão as variações — reza Marc.

Para Ricardo Costa, especialista em segurança da Symantec, tempo de resposta é problema menor, simplesmente porque o antivírus, sozinho, não dá conta das ameaças.

— Há uma convergência grande de ameaças e o tempo de resposta vai variar conforme o tipo de ameaça. Tem ações que levam segundos, outras levam dias. Antivírus com res-

posta rápida é importante mas mais importante é pensar antes, é prevenir, conter o ataque antes que ele aconteça — diz.

Caso aconteça, mesmo as fabricantes que ficarem na lanterna não deixarão os clientes na mão: um acordo exige que, quando o fabricante A descobre uma vacina, ele tem 24 horas para dar o remédio para seus clientes. Findo o prazo, ele deve passar a vacina para os concorrentes, de graça e sem divulgação. ■

Divulgação/F-Secure