EDIÇÃO LARISSA SANTANA (*lasantana@abril.com.br*)

Escola de hackers

O austríaco George Ledin quer nos livrar dos vírus de computador. A receita dele: ensinar seus alunos a fazer os próprios softwares de ataque. **POR INARA CHAYAMITI**

Todos nós – você, seus amigos, o governo e inclusive os jornalistas e designers da SUPER – estamos completamente indefesos na disputa com os vírus que atacam computadores. Os programas que usamos para combater a invasão são como vacinas vencidas, que funcionam apenas contra vírus antigos e não causam nem arranhão nas 15 mil novas versões que surgem a cada semana. É o que diz o professor George Ledin, do curso de pós-graduação em *malware* (*malicious software*, ou "software malicioso" em português) da Universidade Sonoma State, da Califórnia. Ledin está recrutando seus alunos para criar softwares de ataque dentro do laboratório da universidade. A ideia é que a iniciativa – ainda única nos EUA, segundo o professor – seja replicada por outros e inicie um movimento de pesquisa sobre o tema. Só assim teríamos agilidade para acompanhar os movimentos dos hackers, sejam eles adolescentes ou especialistas a serviço de governos. (Sim, os vírus já são usados até para espionagem entre países.) Ainda que fiquem presas em laboratório, as criações caseiras da turma de Ledin não agradaram aos fabricantes de antivírus. As empresas o chamam de traidor e ameaçam não contratar seus alunos. Ledin falou sobre o assunto à SUPER, direto do campus da Sonoma State, na cidade de Rohnert Park.

Por que ensinar alunos a criar vírus?

Não devemos viver num mundo em que o conhecimento esteja apenas nas mãos daqueles que o usam com más intenções. Ao contrário do que se pensa, o conhecimento sobre a produção de vírus não é perigoso. Imagine como seria, por exemplo, se só a indústria farmacêutica entendesse as bactérias. Deixar de ensinar médicos e enfermeiras porque alguns deles poderiam matar seus pacientes seria ridículo.

Mas é preciso que eles criem os programas para entendê-los?

Não é assim em qualquer outra área? Se você quer saber de futebol, precisa jogar, não apenas observar. Nas pesquisas com ▸

Foto Roger Mamer **Ilustração** Firmorama

vírus biológicos, os alunos têm atividades em laboratório. Por que não no caso dos vírus de computador? Simular um ataque ajuda a descobrir como ele funciona. Se você perguntar a usuários de computador se eles são capazes de identificar um vírus, a maioria não tem nem ideia de como começar. A solução para isso é a educação. Infelizmente quase não há estudos, teorias, conferências ou livros sobre a produção de vírus. Pior ainda, não há aulas. Sou o único professor nos EUA que ensina isso. Sistemas operacionais e navegadores têm sido estudados por anos, mas o conhecimento sobre vírus se transformou em um tabu. Estudar e ensinar esse assunto da maneira mais aberta possível pode aumentar a segurança que todos nós temos contra os ataques.

"Nenhum dos vírus que meus alunos fizeram foi identificado por um antivírus. Isso é assustador, pois meus alunos são iniciantes e fazem programas nada sofisticados. Imagine do que especialistas são capazes."

Enquanto deixávamos de produzir conhecimento, os hackers se sofisticavam?

No passado, lidávamos com o tipo de vírus que causa danos visíveis. Agora sofremos ataques sem nem perceber. Um vírus pode se instalar em seu computador e dele mandar spams toda semana sem que você note. E não são apenas os hackers. Muitos classificam os ataques como ações de adolescentes, mas há uma ameaça maior por parte de profissionais treinados que trabalham para governos como os de China e Rússia. Eles enviam vírus a órgãos como o Pentágono para observar as ações de outros países. Isso é perigoso, pois gera uma guerra de computadores pelo mundo todo. Tenho certeza de que alguém do governo americano está lendo toda a comunicação do presidente do Brasil neste momento. E de que alguém está lendo as mensagens de Barack Obama no Brasil. Mas isso não se tornará público. É secreto e não pode ser pesquisado. Enquanto a internet foi formada pela colaboração de universidades, professores, estudantes, pesquisadores, entre outros, o estudo dos vírus ficou concentrado dentro de agências de espionagem, das Forças Armadas e de organizações governamentais secretas.

Então os vírus podem se tornar armas em uma guerra cibernética?

Sim, e isso já está acontecendo. O governo americano, por exemplo, sofre uma média de 10 mil ataques por dia. Esses vírus não estão interessados diretamente em você, e sim nos e-mails do presidente Lula, por exemplo. Ocasionalmente, isso se torna público e vira um escândalo. Aconteceu durante as eleições dos EUA, quando um adolescente do Tennessee leu o e-mail da candidata à Vice-Presidência pelo Partido Republicano, Sarah Palin. Há pessoas especializadas em ler e-mails de presidentes de todos os países.

Se segurança na internet é assunto de Estado, o que o governo deveria fazer para conter a proliferação dos vírus?

O governo deveria apoiar o ensino e a pesquisa aberta. Não deve fazer o que a China faz, por exemplo, que é filtrar o acesso à internet. A única coisa que pode proteger você totalmente dos vírus é desconectar-se, mas isso não é uma alternativa interessante. A melhor solução é permitir que as pessoas que estudam para se tornar profissionais de computação conheçam o máximo possível sobre vírus. Assim, teremos armas mais potentes contra os ataques.

Os ataques a computadores de pessoas comuns também estão mais sofisticados?

Sim. Há um novo programa malicioso que está atacando o *Facebook* e outras redes sociais. Isso é um problema difícil de resolver, pois as pessoas confiam em seus amigos. Como há muita gente nas redes sociais e a comunicação entre os usuários é rápida, as consequências são mais graves. As pessoas também deveriam ter consciência de que tudo o que fazem na internet pode ser visto por alguém. Nada é privado. O ideal seria que as pessoas tratassem seus computadores como algo público, porque na verdade ele pode virar público a qualquer momento. Se você se tornar importante algum dia, alguém por aí vai querer rever o que você andou fazendo no computador – e isso pode significar o fim da sua carreira.

Os pacotes de antivírus hoje no mercado não são suficientes para nos proteger desses ataques?

Não. Todos os pacotes produzidos por empresas trabalham com uma base de dados que identifica alguns tipos de vírus. Mas eles reconhecem apenas vírus antigos. O que fazemos nas minhas aulas comprova isso. O primeiro experimento dos meus alunos é instalar um antivírus e colocar um cd com 100 mil vírus diferentes no computador. O que acontece? O antivírus detecta que existem programas maliciosos, porque reconhece alguns deles em sua base de dados. Essa identificação acontece graças ao que chamamos de assinatura do vírus, ou seja, características do programa que já são conhecidas pelas empresas. Assim, o vírus é enviado para quarentena ou removido. O problema é que, se o aluno troca apenas al-

guns bits da assinatura de um desses vírus antigos, a base de dados não o reconhece mais. Por isso, não basta confiar em programas que esperam que vírus velhos continuem circulando por aí. Há novas versões surgindo a cada dia, e nenhum desse pacotes que conhecemos hoje pode identificá-las.

Os programas de atualização vendidos pelas empresas não dão conta disso?

As companhias avisam quando os upgrades, ou as atualizações, são necessários. Mas você paga por essa renovação. Isso é um ótimo negócio para as empresas. Não é preciso trabalhar muito e milhões de pessoas vão lhe mandar dinheiro. Algumas dessas companhias são as mais lucrativas no mercado de computadores, e conseguem isso apenas vendendo vacinas vencidas. Se eu lhe perguntar o nome de empresas de browsers ou processadores, você se lembrará de 2 ou 3. No setor de antivírus, existem mais de 40 conhecidas. Por que isso? Porque trabalhar com antivírus é rentável. É como se uma companhia farmacêutica vendesse uma pílula que não cura. As pessoas pensam que estão a salvo quando compram os pacotes, mas na verdade não estão.

Você passou a ser visto como um inimigo pelas fabricantes de antivírus por causa dessas ideias.

Não é meu objetivo atacar as companhias. Eu simplesmente digo que elas não sabem o que estão fazendo, ou, se sabem, mantêm isso em segredo. Tenho amigos dentro dessas empresas que não me contradizem, mas afirmam que estão fazendo novas pesquisas, baseadas no comportamento do vírus e não só meramente na base de dados de assinaturas. É também o que eu e meus alunos estamos fazendo. A diferença é que as companhias fazem isso secretamente em seus próprios laboratórios. Nenhum dos vírus que meus alunos fizeram até hoje jamais foi identificado por algum dos pacotes antivírus que estão no mercado. E isso é muito assustador, pois meus alunos são iniciantes e fazem programas nada sofisticados. Imagine então do que especialistas em agências de espionagens são capazes.

Como garantir que seus alunos não se tornarão hackers no futuro?

Isso não é possível, assim como não se pode garantir que estudantes de química não fabricarão substancias tóxicas, por exemplo. Mas tenho duas políticas para evitar que isso aconteça. A 1ª é que tudo o que criamos fique fechado no laboratório. A 2ª é que façamos constantemente debates sobre como manter a ética ao lidar com os nossos programas.

Mas algumas companhias de antivírus consideram seus alunos uma ameaça. Chegaram a dizer que nunca os contratariam.

É verdade, elas disseram isso. Mas muitas empresas e até o governo americano já aceitam meus alunos. Todos perceberam que um boicote como esse seria um grande erro. É como se eles não quisessem empregar quem realmente sabe fazer as coisas. E eu acredito que isso não é lá muito esperto.

Há alguma lei que proíbe a disseminação do conhecimento sobre vírus?

Sim, a Lei de Direitos Autorais do Milênio Digital. Essa lei proíbe que se faça engenharia reversa, que é algo como desmontar uma máquina para descobrir como ela funciona. Por exemplo, se você fabrica automóveis e compra um de outra empresa, você pode analisar como sua concorrência faz esse trabalho. Isso é proibido para softwares, eles não podem ser desmontados. É por isso que empresas desse setor mantêm laboratórios na Bulgária ou na Romênia, pois nos EUA isso não é permitido. Essa é uma lei equivocada, porque precisamos entender como um vírus trabalha. Como você poderia estudar medicina sem pessoas doentes ou se seu hospital tivesse de mandar os pacientes para a Bulgária?

O primeiro passo para intensificar o estudo de vírus seria mudar essa lei?

Seria. A Microsoft, por exemplo, tem muitas vulnerabilidades, e eu não posso criar soluções para arrumá-las, pois sou proibido pela lei. É como se você comprasse um carro com um problema no motor que você sabe consertar sozinho, mas não pudesse arrumar. Dessa forma, a regulamentação acaba protegendo os criadores de programas maliciosos.

Que outros benefícios a democratização do conhecimento poderia nos trazer?

Hoje os vírus de computador são mais simples do que os biológicos, mas é inevitável que eles fiquem mais sofisticados. Quando isso acontecer, os vírus de computador nos ajudarão a entender o funcionamento dos que infectam nosso corpo. E eu prefiro que essa seja uma pesquisa aberta, conduzida por uma universidade, e não fechada a sete chaves. S

George Ledin

- Tem 62 anos, é viúvo e tem um casal de filhos.
- Nasceu na Áustria, mas mudou-se com a família para Caracas, na Venezuela, quando tinha apenas 1 mês de idade.
- Formou-se engenheiro matemático pela Universidade da Califórnia, em Berkeley. É também bacharel em direito pela Universidade de São Francisco.
- Toca piano nas horas vagas. Villa-Lobos é um de seus compositores preferidos.
- As duas coisas que mais o irritam são pessoas ignorantes com poder e desigualdade entre sexos.
- Tem vontade de assistir a *Dona Flor e Seus Dois Maridos*, filme de Bruno Barreto.