

Sensores monitoram atividades maliciosas na rede

Para identificar varreduras, ataques e ferramentas utilizadas em invasões de máquinas, existem dois recursos computacionais: as honeynets e as redes distribuídas de honeypots. As honeynets são redes de pesquisa que abrigam apenas atividades maliciosas. Essas redes usam honeypots de alta interatividade, isso significa que os atacantes podem assumir o controle da máquina invadida. As redes distribuídas de honeypots têm baixa interatividade porque usam apenas emulações das aplicações e dos sistemas operacionais reais. Quando um honeypot

de baixa interatividade é atacado, não está sendo invadida uma máquina de verdade, mas um computador de “faz de conta”. Os honeypots de baixa interatividade são inseridos em redes de produção com alto valor agregado como universidades e centros de pesquisa.

A maioria dos hackers não percebe que as honeynets são redes de teste e invadem as máquinas comprometidas para atacar outros computadores. Uma das características desse tipo de rede é a facilidade que o invasor tem para entrar e a dificuldade que encontra ao tentar sair. A vantagem das honeynets em

relação às redes distribuídas de honeypots é que todas as atividades maliciosas podem ser monitoradas. É possível se observar, entre outras coisas, as ferramentas utilizadas pelos atacantes, verificar se os invasores estão conversando via chats e descobrir a motivação dos ataques.

Nas redes distribuídas de honeypots não é possível capturar todas as informações dos ataques porque não há muita interatividade, mas como os honeypots estão numa rede de produção, é fácil identificar que ataques estão sendo dirigidos a redes de alto valor.

Consórcio Brasileiro de Honeypots detecta ataques no país

Desde março de 2002, o Brasil conta com uma honeynet que detecta atividades de atacantes em redes conectadas à Internet. O projeto Honeynet.BR é uma iniciativa do Instituto Nacional de Pesquisas Espaciais (INPE) e do Grupo de Resposta a Incidentes para a Internet brasileira, NIC BR Security Office (NBSO). O projeto evoluiu e se transformou no Consórcio Brasileiro de Honeypots, coordenado pelo NBSO e pelo Centro de Pesquisa Renato Archer (CenPRA), instituição do Ministério da Ciência e Tecnologia na área de Tecnologia da Informação.

O consórcio tem o objetivo de aumentar o nível de segurança do espaço virtual brasileiro por meio da detecção de atividades maliciosas, correlação de eventos e determinação de tendências de invasões. A idéia é fazer um mapeamento dos ataques contra a Internet brasileira.

Por enquanto o consórcio tem estatísticas sobre os serviços mais atacados, a procedência dos ataques e os endereços das máquinas que são utilizadas para um maior número de invasões. Também já é possível identificar os países de onde partem os ataques, isso não quer dizer que o atacante seja o dono de determinada máquina, mas que, provavelmente, controla

aquele computador. Em 100% dos casos o hacker utiliza o IP de outra máquina.

Os dados coletados até agora estão sendo distribuídos entre as instituições que fazem parte do consórcio. Segundo o pesquisador Antônio Montes do CenPRA, a intenção é divulgar as estatísticas para o público em geral já em 2005. Os sensores que estão na rede brasileira dão uma idéia do tipo de ataques que estão sendo realizados. A pesquisa é feita por amostragem, já que é impossível processar todas as informações devido à quantidade enorme de dados. Como a rede é bastante distribuída, a amostra é representativa. Montes lembra que estatísticas divulgadas por sites ou jornais muitas vezes são extrapolações porque são generalizações de um pequeno domínio. Para o pesquisador, amostragem é como previsão do tempo, não se pode fazer uma afirmação categórica.

Outra missão do consórcio é determinar tendências, ou seja, observar as vulnerabilidades dos sistemas e os serviços que são mais atacados para investir em ferramentas de segurança. Os malwares e worms coletados são enviados para um site mantido por todas as empresas de antivírus. Ao ser identificado um malware desconhecido, as empresas desenvolvem uma vacina.

Brasil é um dos integrantes da Honeynet Research Alliance

O Honeynet Project, criado em 1999 pelo americano Lance Spitzner, foi pioneiro no estudo do comportamento dos invasores de uma rede para o desenvolvimento de ferramentas e sistemas de defesa. O projeto se transformou na Honeynet Research Alliance, organização internacional que reúne diversos consórcios de várias partes do mundo.

Segundo Antônio Montes do CenPRA, no Brasil há esforços isolados do mesmo nível dos provenientes do exterior. A diferença é que em outros países o trabalho é mais difundido. Para o pesquisador, um dos grandes entraves brasileiros é a falta de pessoal capacitado. Nos Estados Unidos, por

exemplo, 50 universidades participam do programa de excelência na formação de especialistas em segurança de Sistemas de Informação. “Aqui ainda se tem a idéia de que segurança pode ser feita por um “hackerzinho”, declara Montes.

No Brasil, um hacker que baixou da Internet alguns programas e invadiu um site já é considerado um especialista e vai trabalhar como consultor de segurança em uma empresa. O resultado é que são contratadas pessoas com pouco conhecimento de redes e de sistemas operacionais, que não têm condições de ter uma atuação eficaz.

O projeto Honeynet tem ajudado a formar

massa crítica na área. As pessoas envolvidas acompanham ataques reais e tomam conhecimento das vulnerabilidades existentes. É claro que a iniciativa não dispensa a necessidade de boas universidades. “A falta de pessoas especializadas é muito grande e em decorrência disso a situação da segurança no Brasil é muito ruim”, explica Montes.

O governo federal, por meio do Gabinete de Segurança Institucional, está iniciando um processo de conscientização de funcionários na Administração Pública Federal com relação a problemas associados à segurança de Sistemas de Informação.

Para saber mais, visite: <http://www.honeypots-alliance.org.br/>.