



Sobre o **Symantec Internet Security Threat Report**

O Symantec *Internet Security Threat Report* apresenta uma atualização semestral das atividades das ameaças na Internet . Nele se incluem as análises dos ataques baseados em redes, uma revisão das vulnerabilidades conhecidas, destaques sobre códigos maliciosos e sobre outros riscos à segurança. Este sumário do atual *Internet Security Threat Report* pode alertar os leitores sobre as ameaças iminentes e as atuais tendências, além de oferecer algumas recomendações para a mitigação e a proteção contra as questões levantadas. Este volume cobre o semestre iniciado em 1º de julho e findo em 31 de dezembro de 2004.

Com mais de 20.000 sensores monitorando as atividades de rede em mais de 180 países pelo Symantec DeepSight™ Threat Management System e pelo Symantec™ Managed Security Services, a Symantec estabeleceu uma das fontes de dados mais abrangentes no mundo sobre as ameaças à Internet. Além disso, a Symantec coleta dados sobre códigos maliciosos, bem como de spyware e adware, reportados por mais de 120 milhões de sistemas clientes, servidores e gateways que implementaram os produtos antivírus da Symantec. A Symantec também mantém uma das bases de dados mais abrangentes no mundo sobre vulnerabilidades à segurança, cobrindo mais de 11.000 vulnerabilidades que afetam acima de 20.000 tecnologias de mais de 2.000 fornecedores. Somado a essa base de dados sobre vulnerabilidades, a Symantec mantém o BugTraq, um dos fóruns mais populares de divulgação e discussão das vulnerabilidades na Internet. Por fim, as Sondas de Rede Symantec, um sistema com mais de 2 milhões de contas-iscas, atrai e-mails em 20 diferentes países ao redor do mundo, permitindo à Symantec medir a atividade mundial de spams e phishing. Esses recursos dão aos analistas da Symantec uma fonte de dados sem paralelo, na qual podem identificar as tendências emergentes na atividade dos ataques e dos códigos maliciosos.

O Symantec *Internet Security Threat Report* é fundamentado principalmente na análise que os especialistas fazem sobre dados reais. Baseado na experiência e no know-how da Symantec, o *Internet Security Threat Report* rende um ensaio extremamente informado sobre as atividades das ameaças atuais na Internet. Ao publicar no *Internet Security Threat Report* as análises da discussão sobre as atividades em torno da segurança na Internet, a Symantec espera fornecer à comunidade de segurança da informação os elementos de que precisam para proteger, hoje e no futuro, seus sistemas com eficiência.

Sinopse Geral

Como já notado no *Internet Security Threat Report* anterior, as vulnerabilidades das aplicações web continuam a ser uma séria ameaça. As aplicações web são alvos populares porque elas apresentam uma ampla implantação e podem permitir aos hackers circunscrever as medidas tradicionais de segurança, como os firewalls. Elas criam uma séria preocupação à segurança porque podem permitir que os atacantes acessem informações confidenciais sem ter de comprometer um servidor em particular. Quase 48% de todas as vulnerabilidades documentadas entre 1º de julho e 31 de dezembro de 2004 são vulnerabilidades de aplicações web.

Entre 1º de julho e 31 de dezembro de 2004, a Symantec documentou 1.403 novas vulnerabilidades, que perfazem mais 54 novas vulnerabilidades por semana, ou quase oito novas vulnerabilidades por dia. Dessas vulnerabilidades, 97% foram consideradas de moderada ou alta severidade, o que significa que a exploração bem-sucedida da vulnerabilidade pode resultar em um comprometimento parcial ou completo do sistema visado. Além disso, 70% foram consideradas de fácil exploração, o que significa que ou nenhum código personalizado era requerido para explorar a vulnerabilidade ou que o código necessário já estava disponível ao público. Para agravar esse problema, cerca de 80% de todas as vulnerabilidades documentadas no período do relatório são exploráveis remotamente, o que, provavelmente, aumenta o número de hackers em potencial.

No volume anterior do *Internet Security Threat Report*, a Symantec previu que o phishing também emergiria como uma séria questão à segurança. Ao longo dos últimos seis meses, essa preocupação se concretizou. Phishing é um método de roubar informações confidenciais, como senhas, números de cartões de créditos e outros dados financeiros. Isto é uma séria ameaça aos consumidores e às empresas. Utilizando sofisticados métodos de engenharia social, os hackers induzem os usuários a revelar suas informações confidenciais. Entre maio de 2003 e maio de 2004, as perdas incorridas pelos bancos e operadoras de cartões de crédito nos EUA resultantes de fraudes ligadas ao phishing foram estimadas em 1,2 bilhão de dólares. Entre 1º de julho e 31 de dezembro de 2004, a Symantec detectou 10.310 novos ataques de phishing. Além disso, no fim de dezembro, os filtros antifraude do Symantec Brightmail™ AntiSpam estavam bloqueando, em média, mais de 33 milhões de tentativas de phishing por semana, em contraposição aos, aproximadamente, 9 milhões por semana no começo de julho.

O phishing não é apenas uma ameaça à informação confidencial. Alguns códigos maliciosos são criados com a intenção de roubar informações confidenciais dos computadores comprometidos. Entre 1º de julho e 31 de dezembro de 2004, essas ameaças representaram 54% das 50 principais amostras de códigos maliciosos recebidas pela Symantec, comparadas com 44% no primeiro semestre de 2004 e 36% no segundo semestre de 2003. Isto se deve em parte pelo contínuo uso de Cavalos de tróia, uma ameaça especial à exposição de dados confidenciais. Entre 1º de julho e 31 de dezembro de 2004, os Cavalos de tróia representaram 33% da lista dos 50 principais códigos maliciosos reportados à Symantec.

Durante esse período, houve um aumento significativo no número de variações de vírus e worms baseados no Windows. De 1º de julho a 31 de dezembro de 2004, a Symantec documentou mais de 7.360 novas variações de vírus e worms Win32. Isso representa um aumento de 64% sobre o semestre anterior. Em 31 de dezembro de 2004, o total de ameaças Win32 documentado, e suas variantes, estava se

aproximando de 17.500. Isto força as organizações a atualizarem suas soluções antivírus com uma frequência jamais vista, o que por si coloca mais pressão sobre os recursos atuais.

Para passar um panorama sobre os tipos de informações incluídos no relatório, o restante deste documento destacará um pequeno subconjunto das descobertas preliminares que serão discutidas com mais profundidade na edição de março de 2005.

Destaques

Tendências entre os Ataques

- Pela terceira vez consecutiva, o ataque Microsoft SQL Server Resolution Service Stack Overflow (Estouro de Pinha do Serviço de Resolução do Servidor Microsoft SQL, conhecido anteriormente como Ataque Slammer) foi o mais comum, utilizado por 22% de todos os atacantes.
- As organizações receberam 13,6 ataques por dia, ante 10,6 registrados nos seis meses anteriores.
- Os computadores em rede bot conhecidos diminuíram de 30.000 por dia no fim de julho para menos de 5.000 por dia no fim do ano.
- O Reino Unido tem uma porcentagem mais alta de computadores infectados por bots do que qualquer outro país.
- Os Estados Unidos continuam a ser o principal país de origem dos ataques, seguidos por China e Alemanha.
- O setor de serviços financeiros passou por 16 eventos severos a cada 10.000 eventos de segurança, a maior taxa registrada entre todos os setores.

Tendências entre as Vulnerabilidades

- O tempo entre a descoberta de uma vulnerabilidade e o lançamento de uma exploração a ela associada aumentou de 5,8 para 6,4 dias.
- A Symantec documentou 1.403 novas vulnerabilidades, um aumento de 13% sobre o mesmo período anterior.

- As vulnerabilidades das aplicações web responderam por 48% de todas as vulnerabilidades descobertas, as quais, na primeira metade de 2004, respondiam por 39%.
- 97% das vulnerabilidades descobertas foram classificadas como de severidade moderada ou alta.
- Durante dos últimos seis meses, foram descobertas 21 das vulnerabilidades que afetam os navegadores Mozilla, comparadas com 13 vulnerabilidades que afetam o Microsoft Internet Explorer.
- 70% das vulnerabilidades reportadas foram consideradas de fácil exploração.

Tendências entre Códigos Maliciosos

- Variantes do Netsky, do MyDoom e do Beagle dominaram as dez principais amostras de código maliciosos em 2004.
- A Symantec documentou mais de 7.360 novos vírus e worms Win32, um aumento de 64% sobre o primeiro semestre do ano.
- Os códigos maliciosos que expõem informações confidenciais respondem por 54% da lista das 50 principais amostras de códigos maliciosos, as quais, no período anterior, perfaziam 44%.
- No fim do período relatado, havia 21 amostras conhecidas de códigos maliciosos para aplicações móveis, quando em junho de 2004 só havia uma.
- Dois bots estavam presentes entre as dez principais amostras de códigos maliciosos comparados com apenas um no mesmo período anterior.
- 4.300 novas variações distintas do Spybot foram relatadas, verificando um aumento de 180% sobre os seis meses anteriores.

Outros Riscos à Segurança

- Nos últimos seis meses de 2004, os programas adware responderam por 5% das 50 principais ocorrências relatadas pelos clientes Symantec, enquanto respondiam por 4% das ocorrências anteriores.
- O Iefeats foi o programa adware mais relatado, respondendo por 36% entre os dez principais adwares.

- O Webhancer foi o programa spyware mais relatado durante a segunda metade de 2004, representando 38% dos relatos entre os dez principais spywares.
- Cinco das dez principais amostras de adware relatadas são instaladas através do navegador web. Nove entre dez programas spyware relatados estão ligados a outro software.
- Entre 1º de julho e 31 de dezembro de 2004, a Symantec detectou 10.310 novos ataques distintos de phishing.
- No fim de dezembro, os filtros antifraude da Symantec estavam bloqueando, em média, mais de 33 milhões de tentativas de phishing por semana, ao passo que, no começo de julho, bloqueavam aproximadamente 9 milhões por semana.
- A Symantec observou um crescimento de 77% nos spams, para empresas cujos sistemas estavam monitorando spams.

Tendências Futuras

- A Symantec acredita que aumentará o uso de bots e das redes bots para obter ganhos financeiros.
- É esperado que cresça tanto em número quanto em severidade o uso de códigos maliciosos visando dispositivos móveis.
- A Symantec acredita que haverá um aumento nos ataques do lado-cliente que utilizam vírus e worms como métodos de propagação.
- A Symantec espera um aumento nos ataques ocultos embutidos no conteúdo de áudio e vídeo.
- A Symantec espera pesquisadores de vulnerabilidade para aumentar o seu foco no Mac OS.
- A Symantec prevê o aumento dos riscos à segurança associados ao adware e ao spyware. A implementação de legislações para conter esses riscos não deve ser eficaz ou suficiente para, por si, eliminá-los.