



Internet Security Threat Report – Fevereiro de 2005

Dados Regionais – América Latina

OBSERVAÇÕES IMPORTANTES SOBRE ESTAS ESTATÍSTICAS

As estatísticas discutidas neste documento são baseadas nos ataques contra uma amostra abrangente de clientes Symantec. As atividades de ataques foram detectadas pelo Symantec™ Managed Security Services e pelo Symantec DeepSight™ Threat Management System entre 1º de julho e 31 de dezembro de 2004.

O Symantec Managed Security Services e o Symantec DeepSight Threat Management System utilizam recursos automáticos para mapear os endereços IP dos sistemas invasores para identificar o país no qual estão localizados. Entretanto, como os hackers freqüentemente utilizam sistemas comprometidos ao redor do mundo para lançar seus ataques remotamente, o local do sistema invasor pode ser diferente do local do hacker. Apesar das incertezas que isso cria, a Symantec crê que esse tipo de dado é útil para definir um perfil de alto nível dos padrões de ataque globais.

O número de sensores distribuído em cada região varia. Combinadas com diferentes normas de segurança, essas variações podem resultar em diferenças nos dados sobre ataques registrados em cada região. Isto pode obstruir a validade das comparações entre as regiões.

Resumo

Além dos dados coletados para o *Internet Security Threat Report*, a Symantec também fez uma análise sobre os dados de ataques na América Latina. Este relatório regional irá destacar os principais ataques, os principais países de origem e os principais códigos maliciosos visando a região da América Latina. Ele também irá identificar as cidades na América Latina com as maiores porcentagens de computadores infectados por bots.

Entre 1º de julho e 31 de dezembro de 2004, o principal ataque na região foi o Microsoft SQL Resolution Service Stack Buffer Overflow (Estouro de Pilha do Serviço de Resolução do Microsoft SQL). Esse ataque é mais comumente associado com o worm Slammer, que começou a disseminar-se em janeiro de 2003. Entretanto, outros códigos maliciosos, incluindo algumas versões do Gaobot e do Spybot, também utilizam esse ataque para comprometer os sistemas de computador.

Cinco dos dez principais ataques na América Latina utilizam HTTP como vetor de ataque. Conhecidos como ataques de aplicações web, eles visam às aplicações ou serviços que são conduzidos em ou através de HTTP. Esses ataques são preocupantes porque podem permitir ao hacker circunscrever as medidas de segurança de perímetro, tais como firewalls. Eles também fornecem um bom acesso às informações confidenciais das organizações.

Entre 1º de julho e 31 de dezembro de 2004, três dos cinco principais países de origem dos ataques detectados pelos sensores na região da América Latina faziam parte da região. A tendência de computadores atacando sistemas localizados na sua própria região já havia sido observada em volumes anteriores do *Internet Security Threat Report*.

Reconhecendo a contínua ameaça imposta pelas redes bot¹, a Symantec começou a rastrear a distribuição de computadores infectados com bots na região da América Latina. Par tanto, a companhia calculou o número de computadores que se sabe estar infectados por bots e estimou quais cidades possuem as maiores concentrações desses computadores. A identificação dos computadores infectados por bots é importante, já que grandes percentuais de máquinas infectadas podem significar um maior potencial de ataques relacionados aos bots. Isso também indica o nível de consciência sobre patches e segurança

Entre 1º de julho e 31 de dezembro de 2004, as cidades na América Latina com os maiores percentuais de computadores infectados por bots foram São Paulo, Cidade do México e Buenos Aires. A Symantec acredita que há dois fatores que afetam significativamente a distribuição dos computadores infectados por bots: o tamanho populacional e a penetração da Banda Larga na cidade.

As duas amostras de códigos maliciosos mais relatadas na região da América Latina durante a segunda metade de 2004 foram bots: Gaobot e Spybot. O fato mais notável, nos códigos maliciosos específicos à América Latina, foi a presença dos Cavalos de tróia para roubo de senha Banpaes² e Bancos³, entre as dez principais amostras de códigos maliciosos.

¹ Bots (abreviação inglesa para robô) são programas que são instalados secretamente na máquina do usuário para permitir que um usuário não autorizado controle o computador remotamente. Eles permitem que um atacante controle remotamente o sistema visado por meio de um canal de comunicação, como o IRC. Estes canais de comunicação são usados para permitir ao atacante remoto controlar um grande número de computadores comprometidos por meio de um canal único e confiável em uma rede bot, a qual pode, então, ser usada em ataques coordenados.

² <http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.banpaes.html>

³ <http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.bancos.html>

Maiores ataques

Posição	Ataque	Porcentagem de Endereços IP Atacando	Serviço Afetado
1	Ataque Microsoft SQL Server 2000 Resolution Service Stack Overflow	37%	Serviço SQL Microsoft
2	Ataque Microsoft IIS 3.0 "%2e" ASP Source Disclosure	12%	Servidor Web (HTTP) Microsoft IIS
3	Ataque Generic WebDAV/Source Disclosure "Translate:f" HTTP Header Request	8%	Serviço Web Genérico (HTTP)
4	Ataque Microsoft Windows DCOM RPC Interface Buffer Overrun	7%	Serviço de Compartilhamento de Arquivos e Impressora Microsoft
5	Ataque Microsoft IIS WebDav Lock Method Memory Leak DoS	5%	Servidor Web (HTTP) Microsoft IIS
6	Ataque Generic HTTP Directory Traversal	5%	Serviço Web Genérico (HTTP)
7	Ataque Generic HTTP 'cmd.exe' Request	2%	Serviço Web Genérico (HTTP)
8	Ataque Generic TCP Syn Flood Denial of Service	2%	Negação de Serviço Genérico
9	Codificação de byte limitado utiliza caracteres não ASCII como valores válidos em decodificação UTF-8	2%	Serviço Web Genérico (HTTP)
10	Ataque Microsoft NT NetBIOS NULL Session	1%	Serviço de Compartilhamento de Arquivos e Impressora Microsoft

Tabela 1. Principais ataques na região da América Latina.

Discussão

Para os propósitos deste relatório, os principais ataques foram definidos como porcentagem de endereços de IP, que lançaram a invasão, em relação ao total.

Entre 1º de julho e 31 de dezembro de 2004, o principal ataque na região da América Latina foi o Microsoft SQL Resolution Service Stack Buffer Overflow (Estouro de Pilha do Serviço de Resolução do Microsoft SQL).⁴ Esse ataque, conhecido anteriormente como Ataque Slammer, é geralmente associado a três códigos altamente maliciosos: Slammer, Gaobot e Spybot.

37% dos endereços de IP invasores detectados pelos sensores na região da América Latina realizaram um ataque Microsoft SQL Resolution Service Stack Overflow. Esse ataque pode afetar tanto o Microsoft SQL Server quanto o MSDE (Microsoft Desktop Engine) que está

⁴ Para os propósitos deste relatório, os principais ataques foram definidos como porcentagem de endereços IP, que lançaram o ataque, em relação ao total.

incluído em alguns softwares de terceiros, o que torna desafiante a aplicação de patches em todos os sistemas vulneráveis de uma organização.

A alta posição desse ataque é provavelmente atribuída a dois fatores relacionados ao uso de UDP como mecanismo de transporte. Primeiro, o uso de UDP permite que seja enviado um ataque completo⁵ para cada computador vítima em potencial, independente de o SQL Server estar ou não instalado e em execução. A maioria dos sistemas de detecção de intrusão irá interpretar cada tentativa como um ataque completo, mesmo se o computador de destino não estiver ligado. Segundo, o uso de UDP permite que esse ataque venha de um endereço falsificado, que pode inflar o número de endereços de IP fontes observados. O Slammer não oculta a sua fonte; entretanto, já que o ataque é utilizado agora por outros códigos maliciosos, essa habilidade pode ter sido acrescentada.

Esse ataque é particularmente arriscado para computadores móveis. Se forem infectados fora do perímetro tradicional, eles poderão transferir o código malicioso para dentro do perímetro por meio de VPN ou ao se conectarem diretamente à rede. Uma filtragem no perímetro das portas Microsoft SQL e uma forte política de conformidade podem reduzir significativamente o risco de ser comprometido por esse ataque. .

O segundo ataque mais comum detectado pelos sensores na América Latina durante esse período foi o Microsoft IIS 3.0 "%2e" ASP Source Disclosure (Exposição da Fonte ASP por "%2e" no Microsoft IIS 3.0). Esse ataque visa às aplicações web, manipulando a codificação dos caracteres nos requerimentos HTTP. A nomenclatura desse ataque indica que é um evento mais velho visando o IIS 3.0. A inclusão de caracteres codificados em hexadecimal para manipular um servidor web está se tornando muito mais comum e essa classificação é provavelmente devida a uma velha assinatura detectando um novo ataque. É provável que esse ataque não vise diretamente o IIS, mas, ao contrário, indique a manipulação de outra aplicação web.

Cinco dos principais ataques na região da América Latina durante o período deste relatório são ataques a aplicações web que utilizam HTTP como vetor de ataque. As aplicações web são tecnologias que dependem do navegador para a sua interface com os usuários e geralmente ficam hospedadas nos servidores web. Frequentemente são vistas como um modo conveniente de os usuários compartilharem, criarem ou modificarem conteúdo via Internet por meio de um navegador web. Os ataques às aplicações web são particularmente alarmantes porque podem expor informações publicamente pela Internet. As aplicações web podem permitir a um hacker acessar informações confidenciais nas bases de dados sem ter de comprometer qualquer servidor,. Elas também podem possibilitar que esse invasor circunscreva as medidas tradicionais de segurança de perímetro, tais como um firewall. São ainda particularmente perigosos porque podem permitir a um hacker comprometer toda a rede ao ganhar acesso por meio de um único sistema local. Tipicamente, as vulnerabilidades da aplicação web são visadas por ataques que se aproveitam dos erros de validação de entradas e da manipulação inadequada das requisições submetidas. Isto pode permitir a um hacker executar um código malicioso no sistema-alvo.

⁵ UDP não requer que nenhum tipo de sincronização seja feito antes que o dado seja enviado e aceito pelo serviço alvo. Por contrapartida, um atacante que use TCP precisa passar por uma apresentação em três vias para sincronizar os sistemas antes que os dados sejam enviados; portanto, os ataques baseados por TCP só seriam percebidos se o serviço visado aceitar a conexão. No caso do Udp, o sistema atacante simplesmente envia o ataque completo sem se preocupar se o serviço está escutando.

A proteção das aplicações web pode ser um desafio se uma organização depender primariamente das defesas de segurança de perímetro. As aplicações web fornecem serviço por meio da web, o que torna a filtragem impossível. A natureza flexível e interativa de muitas das aplicações web geralmente significa que os ataques podem ser facilmente modificados para evitar os sistemas tradicionais de detecção de intrusão. A Symantec recomenda aos administradores da segurança que auditem todas as aplicações web que estiverem implementadas na rede, tanto as desenvolvidas internamente quanto as de terceiros.

O terceiro ataque mais difundido detectado pelos sensores na América Latina durante o período foi o Generic WebDAV/Source Disclosure "Translate: f" HTTP Header Request (Genérico de Requisição de Cabeçalho HTTP "Translate: f" WebDAV/Fonte Exposta). Trata-se de um ataque baseado na web que visa o WebDAV, um protocolo de compartilhamento de arquivo que permite modificações de documentos por meio do protocolo HTTP. O ataque é detectado quando qualquer um dos vários worms e vírus se propaga por meio da vulnerabilidade de estouro do buffer do ntdll.dll do Microsoft Windows⁶. Muitos sistemas de detecção de intrusão alertam para ataques quando a vulnerabilidade é explorada remotamente via WebDAV. Esse ataque foi originalmente muito associado ao worm Welchia, que começou a se espalhar em agosto de 2003, pouco depois da disseminação do Blaster. Desde então, outros códigos maliciosos, incluindo o Gaobot e outros softwares de rede bot, têm explorado essa vulnerabilidade.

Principais países de origem

Posição	País	Porcentual de Ataques
1	Estados Unidos	39
2	Peru	10
3	Brasil	7
4	México	6
5	China	6
6	Japão	3
7	Espanha	3
8	França	2
9	Canadá	2
10	Coréia do Sul	2

Tabela 2. Principais países de origem dos ataques visando a região da América Latina.

Discussão

Os estados Unidos foram o país de origem de 39% dos ataques detectados pelos sensores na América Latina. Isto é, provavelmente, devido ao elevado índice de atividade de ataques originada lá, já que os Estados Unidos são o país de origem de 30% dos ataques, como um todo, à Internet nesse período. Os Estados Unidos continuam a ter mais usuários de Internet do que qualquer outro país, o que pode explicar o alto porcentual de ataques lá originados.

Três dos cinco principais países de origem dos ataques visando a América Latina pertencem à região. Eles são Peru, Brasil e México, que respondem por 23% das atividades de ataque na região. A tendência se os ataques se originaram em computadores localizados na mesma região do sistema de detecção já tinha sido observada em versões anteriores do *Internet Security Threat Report*⁷. Isto se deve, provavelmente, pela maior visibilidade que

⁶ <http://www.securityfocus.com/bid/7116>

⁷ Internet Security Threat Report versão V, março de 2004, página 13

uma organização tem em sua área; assim ela torna-se mais atrativa para os atacantes que estão na sua área. Além disso, o uso de um idioma em comum, como o espanhol na América Latina, também pode contribuir para essa tendência.

Principais cidades infectadas com bots

Posição	Cidade	País	Porcentagem de computadores infectados em relação à América Latina
1	São Paulo	Brasil	16%
2	Cidade do México	México	14%
3	Buenos Aires	Argentina	9%
4	Rio de Janeiro	Brasil	7%
5	San Juan	Porto Rico	5%
6	Monterrey	México	5%
7	Santiago	Chile	5%
8	Guatemala	Guatemala	5%
9	Caracas	Venezuela	2%
10	San Salvador	El Salvador	2%

Tabela 3. Principais cidades infectadas por bots na região da América Latina.

Os computadores infectados por bots operam de modo coordenado sob a direção de um hacker e podem chegar a centenas ou milhares. Essas redes coordenadas de computadores podem procurar e comprometer outros sistemas e podem ser utilizadas para realizar ataques de negação de serviço.

Reconhecendo a contínua ameaça imposta pelas redes bot, a Symantec começou a rastrear a distribuição de computadores infectados com bots na região da América Latina (*Tabela 3*). Para tanto, a Symantec calculou o número de computadores que se sabe estarem infectados por bots e estimou quais cidades possuem as maiores concentrações desses computadores. A identificação dos computadores infectados por bots é importante, já que grandes percentuais de máquinas infectadas podem significar um maior potencial de ataques relacionados aos bots. Isso também indica o nível de consciência sobre patches e segurança

30% dos computadores infectados por bots na América Latina estão localizados nas maiores cidades da região, como São Paulo e Cidade do México. Buenos Aires, cidade menor do que as outras na lista, responde por 9% dos computadores infectados por bots. Embora a população real dessa cidade seja menor do que as outras da lista, a população na área urbana circundante é bem maior. Pode ser que a cidade seja identificada como origem mesmo que o computador infectado por bot esteja localizado na área urbana vizinha.

A Symantec acredita que há vários fatores que influenciam a distribuição dos computadores infectados por bots. No *Internet Security Threat Report* (Volume VII, de março de 2005), a Symantec especulou que o número de computadores com Internet de Banda Larga na região é um fator significativo no número de computadores envolvidos em uma rede bot. Da mesma forma, considerações sobre que tipo de indústria se situa na cidade pode também influenciar fortemente o percentual de computadores infectados por bot. Outro fator pode ser a consciência da população sobre segurança e isso pode estar ligado a outros fatores, como a concentração de empregos de alta tecnologia ou ações específicas de marketing ou educativas executadas pelos principais servidores de serviços de Internet em uma cidade. No caso de Buenos Aires, o número de computadores infectados por bots também pode

estar vinculado ao movimento de se fornecer na cidade um melhor acesso de Banda Larga por conexões sem fio; conforme esse projeto avança, o número de computadores infectados em Buenos Aires pode crescer concomitantemente⁸.

Códigos Maliciosos

Posição	Nome
1	Gaobot
2	Spybot
3	Netsky.P
4	Sasser.B
5	Redlof.A
6	Beagle.AB
7	Netsky.Y
8	PWSteal.Banpaes
9	Beagle.AG
10	PWSteal.Bancos

Tabela 4. Dez principais amostras de códigos maliciosos na região da América Latina.

As duas amostras de códigos maliciosos mais relatadas na região da América Latina durante a segunda metade de 2004 foram o Gaobot e o Spybot. O Gaobot⁹ e o Spybot¹⁰ também estão presentes entre os dez mais no mundo, como foi discutido no *Internet Security Threat Report* (Volume VII, de março de 2005). Como eles não requerem a interação do usuário para se propagar, essas ameaças não são afetadas por coisas como diferenças de idiomas, que poderiam limitar a sua propagação. Além de explorar as vulnerabilidades do Windows, ambas as ameaças utilizam um dicionário de senhas comumente empregadas para se conectar a máquinas Windows remotas. Assim que estiverem conectadas, elas se copiam para a máquina e se executam remotamente.

A presença desses bots nas duas posições mais altas indica que o uso de bots continua a crescer na região da América Latina, uma tendência já notada para a Internet como um todo nos volumes anteriores do *Internet Security Threat Report*¹¹. Isto provavelmente se deve à variedade de funções que podem ser realizadas nos computadores comprometidos.

A terceira amostra de códigos maliciosos mais relatada na região da América Latina durante a segunda metade de 2004 foi o Netsky.P¹². Esse worm de envio em massa é uma variante do Netsky, que se envia usando um arquivo com extensão .zip, o que permite a ele evitar as medidas de filtragem. Como os arquivos com extensão .zip são geralmente confiáveis, os usuários finais estão propensos a abrir o arquivo e, inadvertidamente, executar o vírus.

Na América Latina, o desvio mais notável entre as dez principais amostras de códigos maliciosos soltos na Internet é a presença dos Cavalos de tróia para roubo de senha Banpaes¹³ e Bancos¹⁴, que não estão presentes entre os 50 principais códigos maliciosos relatados mundialmente nesse período. Esses Cavalos de tróia são muito específicos à

⁸ <http://www.80216news.com/publications/page356-1175506.asp>

⁹ <http://securityresponse.symantec.com/avcenter/venc/data/w32.hllw.gaobot.gen.html>

¹⁰ <http://securityresponse.symantec.com/avcenter/venc/data/w32.spybot.worm.html>

¹¹ Volume VI (setembro de 2004) <http://enterprisesecurity.symantec.com/content.cfm?articleid=1539>

¹² <http://securityresponse.symantec.com/avcenter/venc/data/w32.netsky.p@mm.html>

¹³ <http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.banpaes.html>

¹⁴ <http://securityresponse.symantec.com/avcenter/venc/data/pwsteal.bancos.html>

região. Eles tentam roubar informações de autenticação em bancos on-line localizados principalmente no Brasil. Por isso, seus autores tentam atrair usuários nessa região para executar os Cavalos de tróia nos seus computadores, já que é mais provável entre eles ter alguém titular de uma conta nas instituições visadas.

Para prevenir a infecção por códigos maliciosos, é crucial empregar as melhores práticas, como é recomendado pela Symantec¹⁵. Os administradores deveriam manter as aplicações de patches sempre em dia, especialmente no caso de computadores que abrigam serviços públicos e são acessíveis através do firewall ou colocados na DMZ, como os servidores HTTP, FTP, SMTP e DNS. Os servidores de e-mail deveriam ser configurados para admitir somente os anexos considerados necessários à empresa. Por outro lado, outros meios podem ser utilizados para as transferências de arquivos, como os servidores de arquivos, FTP ou SSH.

Os usuários finais devem empregar defesa em profundidade¹⁶, incluindo softwares antivírus e firewall. As definições dos antivírus devem ser atualizadas regularmente. Os usuários também deveriam assegurar que seus sistemas estejam atualizados com todos os patches de segurança necessários fornecidos pelo vendedor do sistema operacional. Eles nunca deveriam ver, abrir ou executar qualquer anexo de e-mail, a menos que o anexo seja esperado e venha de uma fonte conhecida e confiável e que o propósito do anexo seja conhecido. As organizações também deveriam lembrar aos usuários a nunca executarem um software que não tenha sido autorizado.

¹⁵ veja o *Internet Security Threat Report*, Volume VII (março de 2005), Apêndice A

¹⁶ A abordagem de segurança na qual cada sistema da rede é protegido no maior grau possível. Isto deveria incluir o emprego de antivírus, firewalls e sistemas de detecção de instrução, entre outras medidas.