

S Y MANTE C ENTERPRISE SE CURIT Y



Relatório Symantec Sobre Ameaças à Segurança na Internet

Tendências para o período de Janeiro a junho de 2007

Volume XII, publicado em setembro de 2007

Resumo executivo

O Relatório de Ameaças à Segurança na Internet da Symantec fornece uma atualização acerca do cenário mundial de ameaças virtuais durante o semestre. Ele inclui a análise de ataques baseados em redes, um resumo das vulnerabilidades conhecidas e destaques de códigos maliciosos. Ele também avalia tendências nas atividades de phishing e spam. Este resumo do Relatório de Ameaças à Segurança na Internet alertará os leitores sobre as tendências atuais e ameaças iminentes. Também oferece recomendações para proteção contra essas ameaças e maneiras de combatê-las. Este volume cobre o período de seis meses compreendido entre 1º de janeiro e 30 de junho de 2007.

A Symantec consolidou um das mais abrangentes fontes de dados sobre ameaças na Internet do mundo. A Rede Global de Inteligência Symantec rastreia ataques por toda a Internet. A rede consiste de mais de 40.000 sensores monitorando a atividade na rede em mais de 180 países. A Symantec também reúne relatórios sobre códigos maliciosos provenientes de mais de 120 milhões de sistemas clientes, servidores e portais que utilizam os produtos anti-vírus Symantec.

A Symantec opera um dos fóruns mais populares para a descoberta e discussão de vulnerabilidades na Internet, a lista BugTraq™ que conta com aproximadamente 50.000 assinantes diretos. Os assinantes contribuem, recebem e discutem diariamente sobre a pesquisa de vulnerabilidades¹. A Symantec também mantém um dos bancos de dados sobre vulnerabilidades mais abrangente do mundo, composto atualmente por informações acerca de mais de 22.000 vulnerabilidades (referentes a mais de uma década) e que afetam mais de 50,000 tecnologias de mais de 8.000 fabricantes. A discussão a seguir, a respeito das tendências de

¹ A lista de correio BugTraq encontra-se hospedada em SecurityFocus (<http://www.securityfocus.com>). Arquivos anteriores estão disponíveis em <http://www.securityfocus.com/archive/1>

vulnerabilidade é baseada em uma análise cuidadosa daqueles dados.

Dean Turner Diretor executivo Symantec Security Response	David McKinney Analista Symantec Security Response	Ollie Whitehouse Arquiteto de segurança – avançado Pesquisa de ameaças Symantec Security Response	Contribuidores David Cowings Gerente de operações Symantec Business Intelligence
Stephen Entwisle Editor sênior Symantec Security Response	Ronald Bowes Analista Symantec Security Response	Zulfikar Ramzan Analista — ameaças avançadas Pesquisa Symantec Security Response	Dylan Morss Gerente Symantec Business Intelligence
Eric Johnson Editor Symantec Security Response	Nicholas Sullivan Analista Symantec Security Response	Jim Hoagland Diretor Engenheiro de Software Symantec Security Response	Shravan Shashikant Diretor de inteligência em negócios Analyst Symantec Business Intelligence
Marc Fossi Analista Symantec Security Response	Candid Wueest Analista Symantec Security Response	Chris Wee Gerente, desenvolvimento Symantec Security Response	
Joseph Blackbird Analista Symantec Security Response			

Finalmente a Symantec Probe Network, um sistema formado por mais de dois milhões de contas-chamariz, atrai mensagens de e-mail provenientes de 20 países diferentes em redor do mundo, permitindo que a Symantec possa medir a atividade global de phishing e spam. Esses recursos dão aos analistas da Symantec incomparáveis fontes de dados com os quais eles podem identificar tendências emergentes em ataques e atividades de códigos maliciosos. A Symantec também reúne informações sobre phishing através da Rede de Relatório sobre Phish Symantec (Phish Report Network) uma ampla comunidade anti-fraude formada por empresas e usuários domésticos. Os membros da rede contribuem com informações e recebem endereços de websites fraudulentos para que permaneçam alerta e para que possam filtrar os sites através de uma ampla gama de soluções.

O Relatório Sobre Ameaças à Segurança na Internet é baseado principalmente na análise de dados provenientes das diversas fontes por um especialista. Baseado na experiência e conhecimento da Symantec, esta análise embasa um comentário altamente informativo acerca da atividade atual de ameaças na Internet. Ao publicar o Relatório sobre Ameaças à Segurança na Internet, a Symantec espera fornecer às empresas e usuários a informação de que eles precisam para assegurar a proteção de seus sistemas agora e no futuro.

Durante os vários períodos dos relatórios passados a Symantec tem observado uma mudança fundamental no cenário de ameaças. Os atacantes migraram de ataques feitos com o intuito de simplesmente perturbar o usuário ou de outros com finalidade destrutiva para ataques motivados por ganho financeiro. Os atacantes de hoje estão cada vez mais sofisticados e organizados e começaram a adotar métodos similares às práticas tradicionalmente usadas no desenvolvimento de softwares.

No Relatório Sobre Ameaças à Segurança na Internet anterior, a Symantec reportou que redes descentralizadas de atividade maliciosa trabalhavam cooperativamente e estavam começando a aparecer. Além disso, padrões de ameaça regionais distintos estavam começando a emergir. Em resposta a essas ameaças, a Symantec lançou três relatórios adicionais: o Relatório sobre Ameaças à Segurança na Internet na Região da Europa Oriente Médio e África (EMEA); o Relatório sobre Ameaças à Segurança na Internet para a região da Ásia-Pacífico e Japão (APJ); e o Relatório sobre Ameaças à Segurança na Internet para o Setor Governamental, focado nas tendências e ameaças que sejam de interesse específico para os setores de governo e infra-estrutura.²

Pela primeira vez a Symantec fornece um resumo executivo que apresenta os destaques de todos os quatro relatórios descritos acima, de modo a propiciar uma análise mais concisa sobre como o cenário de ameaças tem se desenvolvido. Teve-se também a intenção de chamar a atenção para descobertas-chave que não apenas mostram diferenças regionais, mas que mostram como a atividade nessas regiões é tanto um reflexo como uma contribuidora dos padrões de atividade maliciosa global.

Hoje o cenário de ameaças está mais dinâmico do que nunca. Conforme medidas de segurança são desenvolvidas e implementadas para proteger computadores de usuários e de empresas, os atacantes rapidamente adaptam novas técnicas e estratégias para burlar tais medidas. As mudanças que se seguiram têm sido evidentes durante os primeiros seis meses de 2007. Baseando-se nos dados coletados durante o período, a Symantec tem observado que o cenário atual de ameaças à segurança na Internet caracteriza-se por:

- crescente profissionalização e comercialização de atividades maliciosas
- ameaças são, cada vez mais, feitas sob medida para regiões específicas
- número crescente de ataques em múltiplos estágios
- atacantes exploram primeiro entidades da confiança do usuário para depois chegar até o próprio usuário
- convergência dos métodos de ataque

O restante deste resumo executivo explorará estes conceitos em maior profundidade. Também discutirá as implicações das tendências para usuários finais e organizações. Onde for possível, esta discussão também incluirá as estratégias necessárias para que usuários domésticos, administradores e empresas possam proteger-se contra essas ameaças.

Crescente profissionalização e comercialização de atividades maliciosas

Conforme os ataques têm se tornado mais voltados para a obtenção de lucro, muitos aspectos deles tornaram-se profissionais e comerciais. Esse é um sintoma do florescimento de uma economia paralela. No volume IX do Relatório de Ameaças à Segurança na Internet (março de 2006), a Symantec previu que a troca de códigos maliciosos em fóruns populares tais como IRC, web sites e sites de leilão virtual no mercado negro continuaria a crescer³. Enquanto que essa previsão tem se confirmado, a taxa de crescimento excedeu a maioria das previsões. Para atender às necessidades daquilo que se tornou uma atividade criminosa de muitos bilhões de dólares⁴, o desenvolvimento e a distribuição de muitas atividades maliciosas tornou-se profissional e comercial nos últimos dois anos.

O MPack foi uma das notáveis ameaças à segurança surgidas na primeira metade de 2007. Ele é um kit de

² Setores produtores de infra-estrutura crítica incluem telecomunicações, indústria, serviços financeiros, produção militar, saúde, transportes, governo, aeroespacial, legal, biotecnológico e farmacêutico, agricultura e de aplicação da lei.

³ Relatório Symantec de Ameaças à Segurança na Internet, Volume IX (março de 2006): http://eval.symantec.com/mktginfo/enterprise/white_papers/entwhitepaper_symantec_internet_security_threat_report_ix.pdf : p. 19

⁴ <http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf>

ferramentas comercialmente disponível no mercado negro que pode explorar vulnerabilidades de browser e do lado cliente contra usuários que visitem um web site malicioso ou comprometido⁵. A Symantec acredita que o MPack tenha sido desenvolvido profissionalmente. Além do mais, há evidências de que o MPack estava a venda na rede por US\$1,000.⁶

Outra indicação da comercialização de atividade maliciosa foi a emergência de kits de ferramentas de phishing. Um kit de ferramentas de phishing é um conjunto de scripts que permitem que um atacante estabeleça automaticamente web sites de phishing, capazes de imitar os sites verdadeiros de diferentes marcas, incluindo as imagens e logotipos associados com aquelas marcas. Esses scripts também ajudam a gerar mensagens de e-mail de phishing correspondentes.

Kits de phishing começam a ser usados amplamente. Um indicador de um kit de ferramentas de phishing é a hospedagem de um número de websites de phishing em um único endereço IP. Durante a primeira metade de 2007, 86% de todos os websites de phishing relatados à Symantec estavam hospedados em apenas 30% dos endereços IP de phishing. Além disso, observando de perto os três kits de phishing mais usados, constatamos que eles sozinhos foram responsáveis por 42% de todos os ataques de phishing detectados na primeira metade de 2007 (figura 1).

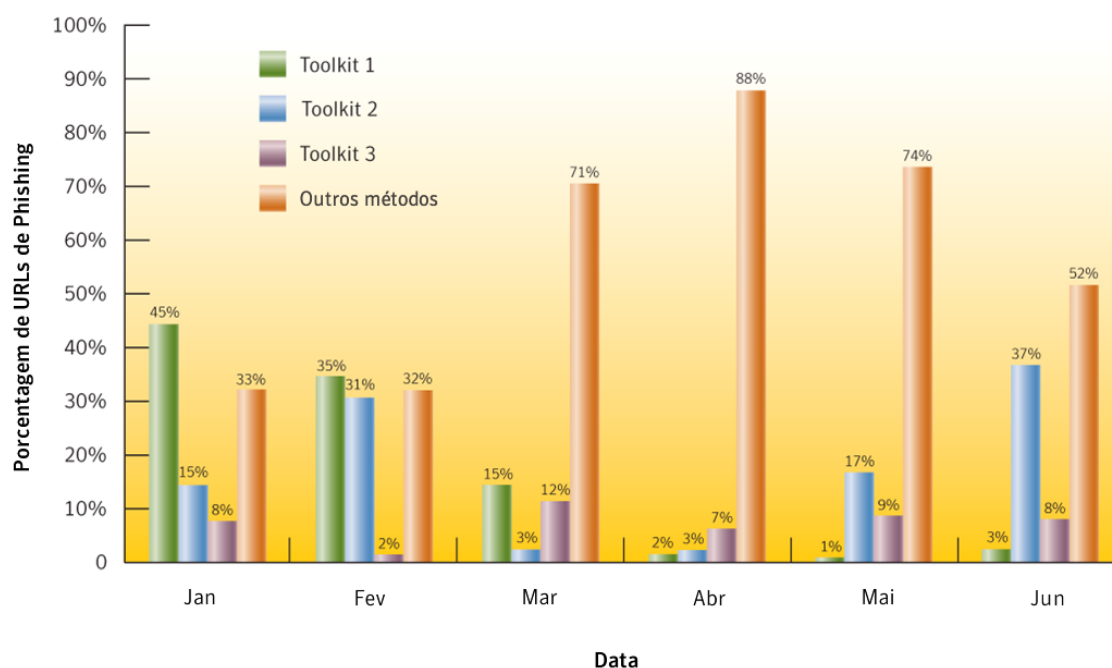


Figura 1. Uso de kits de ferramentas de phishing automatizados, Janeiro – Junho 2007

Fonte : Symantec Corporation

Outra evidência que apóia a crença da Symantec de que a atividade maliciosa está se profissionalizando é a presença de um crescente número de servidores informais. Servidores informais são usados por criminosos e organizações criminosas para vender informação roubada, tipicamente para uso posterior em roubos de

⁵ http://www.symantec.com/enterprise/security_response/weblog/2007/05/mpack_packed_full_of_badness.htm

⁶ http://www.symantec.com/enterprise/security_response/weblog/2007/07/mpack_clearance_sale.html

identidade. Estas informações podem incluir números de identificação fornecidos pelo governo, cartões de crédito, cartões de banco e números de identificação pessoal (PINs), contas de usuários e listas de endereços de e-mail.

Durante os seis primeiros meses de 2007, os Estados Unidos foram o principal país em número de servidores informais, respondendo por 64% de todo o total conhecido pela Symantec. A Alemanha teve o segundo maior número de servidores informais durante o período, respondendo por 12% do total mundial. A Suécia ficou em terceiro, com 9% do total mundial de servidores informais.

Durante a primeira metade de 2007, cartões de crédito foram o item mais frequentemente anunciado para venda em servidores de economia informal, totalizando 22% de todos os produtos anunciados (tabela 1). Durante este período a Symantec observou 8.011 cartões de crédito diferentes sendo anunciados para troca em servidores informais. Porém, isso é apenas uma pequena proporção dos cartões de crédito vendidos através da Internet como um todo. 85% dos cartões de crédito postos a venda em servidores informais conhecidos pela Symantec haviam sido emitidos por bancos nos Estados Unidos.

Posição	Item	Porcentagem	Gama de preços
1	Cartões de crédito	22%	\$0.50–\$5
2	Contas bancárias	21%	\$30–\$400
3	Senhas de e-mail	8%	\$1–\$350
4	Mailers	8%	\$8–\$10
5	Endereços de e-mail	6%	\$2/MB–\$4/MB
6	Proxies	6%	\$0.50–\$3
7	Identidade completa	6%	\$10–\$150
8	Scams	6%	\$10/week
9	Números de seguro social	3%	\$5–\$7
10	Shells UNIX® comprometidas	2%	\$2–\$10

Tabela 1. Análise de produtos disponíveis para venda em servidores de economia informal
Fonte: Symantec Corporation

Ameaças cada vez mais feitas sob medida para certas regiões

Os atacantes estão cada vez mais voltando sua atenção para a criação de ameaças de natureza regional. Enquanto que certo grau deste tipo de atividade tenha sempre existido, análises recentes indicam que atacantes estão atualmente mais focados em alvos que compartilhem da mesma linguagem, infra-estrutura e/ou atividade on-line. Enquanto que a atividade de ameaças anteriores era predominantemente global, a expansão de Internet de banda larga em áreas que tradicionalmente não têm sido servidas por conexões de alta velocidade deu aos atacantes novos alvos para a atividade de ataque.

Em volumes anteriores do Relatório de Ameaças a Segurança na Internet, a Symantec observou que um rápido aumento em banda larga coincide com o rápido aumento da atividade maliciosa.⁷ Em parte isso se deve à realidade que novos usuários de banda larga podem não estar cientes das precauções necessárias para proteger seus computadores. Isso também é provável porque provedores de serviço de Internet (ISPs) em rápida expansão tendem a concentrar esforços no atendimento da demanda crescente em detrimento da implementação de medidas de segurança adequadas, tais como bloqueio de portas e filtragem de entrada e

⁷ Por favor, veja Relatório Symantec de Ameaças à segurança da Internet do Governo -ent/papers_white/enterprise/mktqinfo/com.symantec.eval//http43p:pdf.us-en.2006_09_x_report_threat_security_internet_symantec_whitepaper

saída. Com resultante, esses ISPs podem ter infra-estruturas de segurança que sejam subdesenvolvidas para suas necessidades.

Conforme a banda larga amplia-se por novas áreas e desenvolve uma presença regional mais forte, mais alvos em potencial surgem para os atacantes. A regionalização da atividade de ataques é particularmente evidente na distribuição de certos tipos de códigos maliciosos. Durante este período, 44% de todas as infecções em potencial por cavalos de Tróia foram reportadas a partir da América do Norte, enquanto que 37% foram reportadas da região formada pela Europa, Oriente Médio e África (figura 2). Isso é significativamente mais alto do que os 15% relatados da região formada por Ásia-Pacífico e Japão e os 4% provenientes da região da América Latina.

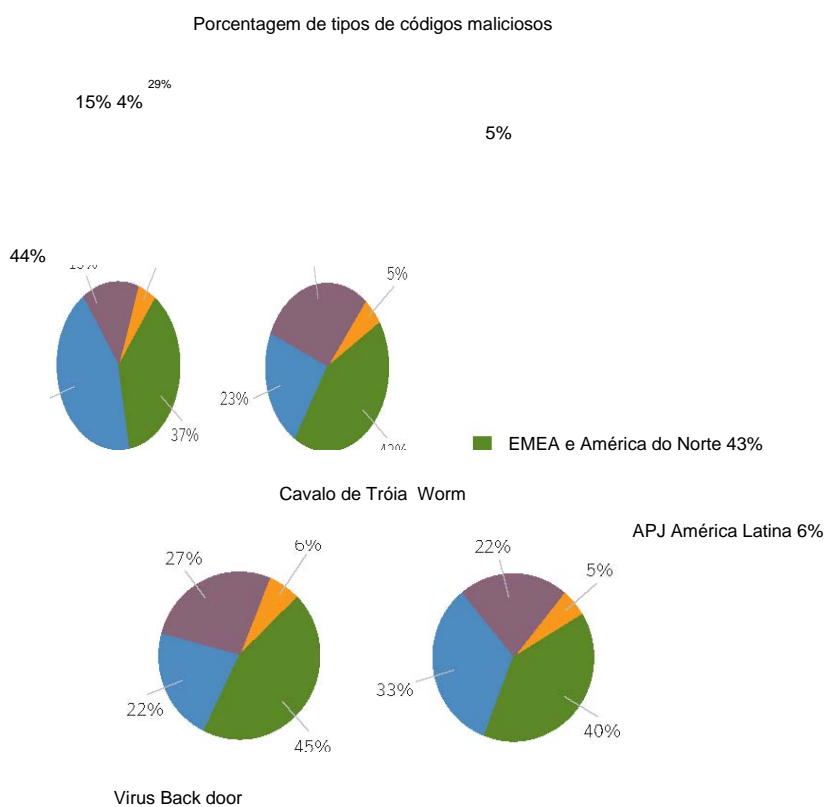


Figura 2. localização de códigos maliciosos por tipo
 Fonte: Symantec Corporation

A concentração de cavalos de Tróia na América do Norte pode ser um sinal indicativo de que empresas e provedores de Internet estão fazendo esforços mais ativos para prevenir a propagação de worms.⁸

Por outro lado, poderia refletir uma decisão consciente dos atacantes de utilizar cavalos de Tróia em reação ao sucesso de defesas de perímetro de rede – tais como sistemas de detecção e prevenção de intrusão (IDS/IPS) e firewalls—que têm sido implementados por provedores de Internet para impedir ataques de worms, mas que tem pequeno efeito em cavalos de Tróia.

Durante este período a região formada pela Europa, Oriente Médio e África (EMEA) respondeu por 43% de

⁸ Tais passos provavelmente incluem bloqueios mais agressivos e filtragem de anexos de e-mail junto ao portal de e-mails a fim de prevenir a propagação de worms de correio eletrônico em massa e também bloqueio de portas para prevenir a difusão de worms de rede.

todas as infecções em potencial causadas por worms, enquanto que a América do Norte sozinha respondeu por 23%. Isso pode indicar que defesas implementadas por provedores de acesso à Internet americanos estejam limitando com sucesso a expansão de worms de rede. Essas defesas tendem a incluir filtragem com antivírus junto ao portal de e-mail para limitar worms de correio em massa.

Uma razão para a distribuição regionalizada de worms é que alguns worms utilizam assuntos e textos relacionados a certas regiões específicas em suas mensagens de e-mail. Por exemplo, o worm Rontokbro, o quinto worm mais comum na região da EMEA durante este período, envia mensagens de e-mail escritas em Indonésio⁹ entretanto, este worm foi encontrado mais frequentemente na Índia do que em qualquer outro país, há muita interação comercial entre a Índia e a Indonésia¹⁰ o que significa que é altamente provável que muitos usuários corporativos na Indonésia comuniquem-se com seus parceiros na Índia através de e-mail. Desde que o Rontokbro envia e-mails para todos os endereços que ele reúne a partir dos arquivos de um computador infectado, parece lógico que este worm tenha sido enviado a muitos usuários indianos a partir de contatos comerciais na Indonésia.

O worm de e-mail em massa Sober.AA foi outro exemplo de praga direcionada a alvos regionais. Ele usou mensagens de e-mail nos idiomas Inglês e Alemão para propagar-se.¹¹ Durante o período deste relatório, o Sober.AA esteve entre os 50 principais tipos de códigos maliciosos na região da EMEA, mas não no mundo inteiro.

Do mesmo modo, muitos dos worms que eram mais freqüentes na região da Ásia-Pacífico e Japão (APJ) durante o período haviam sido feitas sob medida para os usuários daquela região. Por exemplo, o worm Antinny¹² que figurava entre as 10 amostras de códigos maliciosos mais freqüentemente observadas na região, propagou-se através do Winny, um programa japonês de compartilhamento de arquivos (P2P). Outros worms, tais como Looked.BK,¹³ também causaram número significativo de infecções em potencial na região da Ásia-Pacífico e Japão mas não em qualquer outra região. O Looked.BK especificamente desabilitava aplicativos de segurança que enviavam avisos de segurança em Chinês.

A região da Europa, Oriente Médio e África respondeu pela mais alta porcentagem de infecções em potencial por vírus durante o período do relatório: 45% do total. A região da Ásia-Pacífico e Japão respondeu, respectivamente, por 27% e 22% dos vírus, enquanto que a América Latina sozinha respondeu por 6%. A predominância de vírus na região da Europa, Oriente Médio e África pode estar relacionada ao alto número de worms relatados durante este período. Muitos worms estão incorporando um componente viral que faz com que eles sejam classificados tanto como worms quanto como vírus.

Uma razão para o aumento na predileção por ataques regionais é que alguns ataques visam certas atividades em particular que são mais populares em algumas regiões do que em outras. Por exemplo, games on-line tornaram-se um alvo cada vez mais comum para os atacantes. Games on-line parecem ser particularmente populares na região da Ásia-Pacífico e Japão, especificamente na China e Coreia do Sul. Havia 30 milhões de pessoas que jogavam jogos on-line só na China no final de 2006¹⁴.

Durante os seis primeiros meses de 2007, o cavalo de Tróia Gampass apresentou o maior número de infecções em potencial dentre quaisquer outros códigos maliciosos na região da Ásia-Pacífico e Japão.¹⁵ Este

⁹ http://www.symantec.com/security_response/writeup.jsp?docid=2005-092311-2608-99

¹⁰ <http://www.hindu.com/2005/11/24/stories/2005112405871200.htm>

¹¹ http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2007-043010-5416-99

¹² http://www.symantec.com/security_response/writeup.jsp?docid=2003-080817-4045-99

¹³ http://www.symantec.com/security_response/writeup.jsp?docid=2006-112813-0222-99

¹⁴ <http://abcnews.go.com/Technology/wireStory?id=3386396>

¹⁵ http://www.symantec.com/security_response/writeup.jsp?docid=2006-111201-3853-99

cavalo de Tróia visa usuários dos jogos Lineage, Ragnarok Online, Rohan, and Rexue Jianghue. Estes jogos são mais populares na região da APJ do que no resto do mundo.¹⁶ China e Taiwan foram os principais países a relatar infecções em potencial por Gampass durante o período. No total, 84% das infecções em potencial no mundo todo por Gampass durante este período foram originadas naquela região.

Amostra	Tipo	Jogos visados
Gampass	Trojan	Configurável para vários
Lineage	Trojan	Lineage
Dowiex	Vírus, Trojan	World of Warcraft

Tabela 2. As três principais amostras de códigos maliciosos visando sites de jogos on-line
Fonte : Symantec Corporation

Número crescente de ataques em múltiplos estágios

Ataques tradicionais consistem de um único ataque, voltado ao propósito de ganhar acesso não autorizado ao computador ou aos dados armazenados nele. Por outro lado, as técnicas de ataque atuais tornaram-se muito mais sofisticadas. A Symantec tem visto um aumento considerável no número de ataques que utilizam múltiplos estágios. Esses são ataques onde um comprometimento inicial insuspeito é usado para estabelecer um ponto a partir do qual ataques posteriores são lançados.

Em parte, o uso de ataques em múltiplos estágios é indicativo de que os métodos de ataque anteriores – tais como worms de rede em larga escala e ataques de negação de serviço – não são mais eficazes como antes. A fim de ultrapassar fortes defesas de rede, tais como IDS/IPS e firewalls os atacantes adotaram técnicas de ataque mais discretas, tais como ataques em estágios sucessivos que usam cavalos de Tróia para estabelecer um comprometimento inicial. O exemplo mais claro da abordagem em estágios múltiplos são os códigos maliciosos conhecidos como staged downloaders.

Os Staged downloaders, algumas vezes chamados de códigos maliciosos modulares, são ameaças que baixam e instalam outros códigos maliciosos em um computador já infectado. Eles permitem que o agressor possa escolher qual componente deva ser baixado a seguir, de modo a obter a praga que melhor atenda a seus objetivos. Se o objetivo do atacante mudar, ele ou ela pode mudar quaisquer componentes posteriores que devam ser descarregados, de modo a cumprirem as novas tarefas com mais eficiência.

Durante os seis primeiros meses de 2007, 28 dentre os 50 principais códigos maliciosos eram staged downloaders. Embora tenha havido uma ligeira queda em relação ao número prévio de 29 amostras na segunda metade de 2006, durante este período 79% das infecções em potencial por códigos maliciosos eram alguma forma de staged downloader. O novo tipo de código malicioso mais amplamente divulgado durante este período foi um staged downloader conhecido como Peacomm Trojan.¹⁷ O Peacomm baixa e instala outros arquivos, tais como o Mespam¹⁸ e o Abwiz.FTrojans,¹⁹ sendo que este último pode enviar informação confidencial para atacantes remotos e pode ser usado para propagar spam.

¹⁶ http://news.com.com/Consumers+Gaming+their+way+to+growth++Part+3+of+South+Koreas+Digital+Dynasty/2009-1040_3-5239555.html

¹⁷ http://www.symantec.com/security_response/writeup.jsp?docid=2007-011917-1403-99

¹⁸ http://www.symantec.com/security_response/writeup.jsp?docid=2007-020915-2914-99

¹⁹ http://www.symantec.com/security_response/writeup.js?docid=2006-032311-1146-99

Ranking	Amostra	Tipo	Mecanismo de Download
1	Zlob	Cavalo de Tróia	Redireciona o browser para páginas Web maliciosas
2	Vundo	Cavalo de Tróia	Baixa arquivos de endereços remotos
3	Mixor.Q	Worm	Baixa arquivos de endereços remotos
4	Anicmoo	Cavalo de Tróia	Baixa arquivos de endereços remotos
5	Skintrim	Cavalo de Tróia	Baixa arquivos de endereços remotos
6	Metajuan	Cavalo de Tróia	Baixa arquivos de endereços remotos
7	Stration	Worm	Baixa arquivos de endereços remotos
8	Wimad	Cavalo de Tróia	Usa o Gerenciador de Direitos Digitais do Windows Mídia Microsoft® para enganar o usuário e convencê-lo a baixar certos arquivos.
9	Nebuler	Cavalo de Tróia	Baixa arquivos de endereços remotos
10	Secup	Cavalo de Tróia	Mostra avisos de segurança falsos para induzir os usuarios a baixar certos arquivos

Tabela 3. principais staged downloaders
 Fonte: Symantec Corporation

Outro exemplo de ataques em estágios múltiplos é o kit MPack. O MPack, que foi descoberto em maio de 2007, explora vulnerabilidade em plug-ins de browsers da web, especificamente uma vulnerabilidade do QuickTime®,²⁰ um componente ActiveX do WinZip,²¹ e várias outras vulnerabilidades de plug-ins tais como o WebViewFolderIcon Microsoft.²² Durante o período do relatório atual, o kit MPack foi usado para instalar códigos maliciosos em milhares de computadores.²³ Web sites verdadeiros foram comprometidos e modificados de modo a incluir códigos para redirecionar o browser do usuário para um servidor malicioso MPack. O servidor MPack então tentava explorar uma das vulnerabilidades para instalar o primeiro estágio de um multistaged downloader em um computador comprometido.

Amostras de códigos maliciosos que expõem informação confidencial em computadores infectados são outro exemplo da abordagem em vários estágios. Após a infecção inicial, a ameaça pode empregar uma das várias capacidades para enviar informação confidencial ao atacante. Por exemplo, um keystroke logger pode ser usado para gravar informação digitada no teclado de um computador infectado e reportar os dados diretamente ao atacante ou a um servidor sob o controle do mesmo.

Registros de teclado podem conter informações referentes a contas que o usuário tenha digitado enquanto o computador estava infectado; incluem-se aqui credenciais de log-on para diferentes tipos de contas, tais como contas bancárias e para compras on-line, além de contas de provedores de Internet. O atacante pode então usar essas informações como a base para lançar ataques posteriores ou para efetuar roubo de identidade. Ameaças à informação confidencial com capacidade de registro de dados digitados via teclado corresponderam a por 88% das ameaças a informação confidencial durante este período mostrando, portanto um aumento em relação aos 76% constatados na segunda metade do ano passado.

A atividade de phishing visando provedores de serviços de Internet e seus clientes também está relacionada com ataques em estágios múltiplos. 11% das marcas usadas em ataques de phishing na primeira metade de 2007 pertencem a organizações no setor de provimento de serviços de Internet, tornando-o o segundo no ranking durante este período (figura 3).

Conforme notado na versão anterior do Relatório sobre Ameaças a Segurança na Internet, contas de acesso a Internet podem ser alvo valiosos para emissores de phish.²⁴ As pessoas freqüentemente usam as mesmas

²⁰ <http://www.securityfocus.com/bid/21829>

²¹ <http://www.securityfocus.com/bid/21060>

²² <http://www.securityfocus.com/bid/19030>

²³ http://www.symantec.com/enterprise/security_response/weblog/2007/05/mpack_packed_full_of_badness.html

²⁴ Symantec Internet Security Threat Report, Volume XI (March 2007).

credenciais de autenticação (tais como nomes de usuário e senhas) para diversas contas, incluindo contas de e-mail.²⁵ Por isso, a informação compilada através de ataques de phishing pode fornecer acesso a outras contas, tais como contas bancárias on-line.

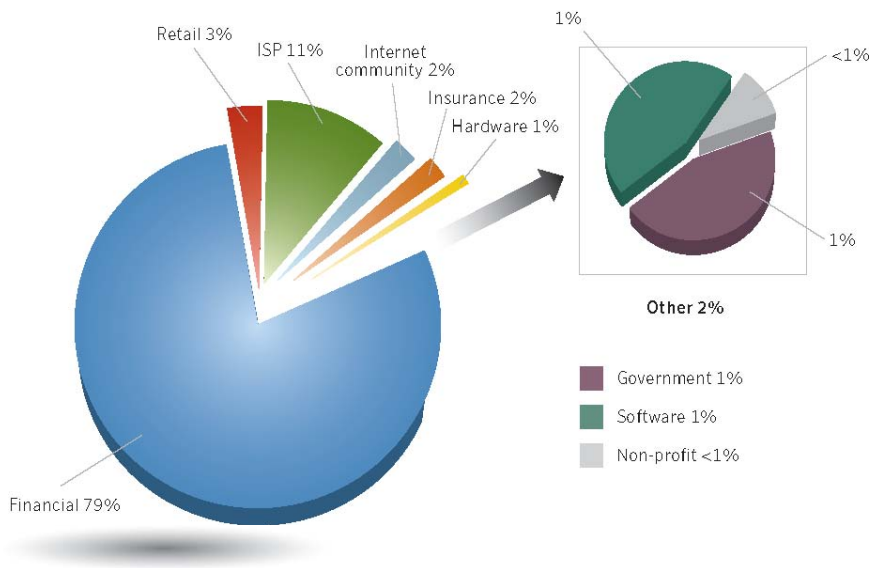


Figura 3 . marcas que sofreram ação de phishing, por setor
Fonte : Symantec Corporation

Em parte o uso de ataques em estágios múltiplos é um passo natural na evolução do objetivo final dos ataques. Durante os últimos dois anos, os ataques têm sido motivados de forma crescente por ganhos financeiros. A maior parte dos ataques é agora dirigida por uma busca de dados ou informações que possam ser usadas diretamente para fraude ou roubo – tais como números de cartões de crédito ou de contas bancárias – ou que possam ser usadas indiretamente para criar as condições necessárias para atividades fraudulentas. O exemplo mais óbvio disso é o roubo de identidade.

Muitos dos ataques em estágios múltiplos que a Symantec detectou foram concebidos para a apropriação indébita de informação confidencial, sendo que em alguns casos isso requer diversos passos. Os métodos de ataque anteriores, tais como worms de rede em larga escala e os ataques de negação de serviço, deixaram de ser eficazes na realização de seus objetivos. Ao invés deles, ataques em vários estágios e em menor escala são mais apropriados. O primeiro estágio desses ataques é frequentemente voltado especificamente para uma região ou para um determinado ramo de atividade, o que aumenta as chances de sucesso da operação. Uma vez que esse primeiro estágio tenha sido executado com sucesso, componentes subseqüentes podem ser baixados para que se obtenha a informação buscada. Já que esses ataques em vários estágios e em pequena escala são motivados por ganhos financeiros, é provável que eles contem com a preferência dos atacantes.

Criminosos exploram sites confiáveis para atingir vítimas

http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xi_03_2007.en-us.pdf : p. 69

²⁵ http://cups.cs.cmu.edu/soups/2006/proceedings/p44_gaw.pdf

Uma das características do cenário de ameaças que emergiu dos últimos anos é que os criminosos não mais procuram ativamente por suas vítimas, ao invés disso, eles procuram atraí-las para si. Assim, ao invés de tentar invadir os computadores de usuários escolhidos como alvos diretamente, os atacantes primeiro comprometem sites e aplicações que sejam da confiança do usuário. Desse modo, assim que um usuário visita aquele site ou utiliza aquela aplicação em particular, o agressor tem finalmente a oportunidade de invadir o PC do usuário, frequentemente ao direcioná-lo a um website malicioso ou ao fazer com que ele baixe um cavalo de Tróia.

Esta tendência tornou-se possível graças ao uso crescente de aplicações Web e tecnologias Web 2.0. Aplicações web são tecnologias que usam um browser para sua interface de usuário, utilizam http como protocolo de transporte e hospedam-se em servidores Web. Exemplos de aplicações baseadas em Web incluem sistemas de gerenciamento, comércio eletrônico (tais como implementações de carrinhos de compra), Weblogs e correio eletrônico baseado na Web.

Tecnologias Web 2.0 dependem em grande parte do modelo de interação *usuário como publicador*. Elas permitem que conteúdo criado pelo próprio usuário possa ser desenvolvido e implementado por grandes grupos de pessoas. Aplicações populares que utilizam tecnologias Web 2.0 incluem sites de relacionamento social e sites wiki, ambos permitem que os usuários possam facilmente colaborar para criar conteúdo.

Durante os últimos anos, conforme as aplicações Web têm sido mais amplamente utilizadas, elas têm sido cada vez mais visadas por atacantes como um simples meio de burlar medidas de segurança na rede, tais como IDS/IPS e firewalls. Sites de relacionamento social têm se mostrado úteis aos atacantes porque eles dão acesso a um grande número de pessoas, muitas das quais confiam implicitamente que aquele site e que seu conteúdo sejam seguros. Os atacantes cada vez mais visam sites de relacionamento social à medida que usuários da rede ficam cada vez mais conscientes dos riscos associados a anexos não solicitados de e-mail e outros engodos.

Os criminosos descobriram que ataques podem ser lançados a partir de sites em que os usuários tendem a confiar, os quais podem ser facilmente comprometidos devido à existência de vulnerabilidades em aplicações web. Durante o período do relatório atual, 61% de todas as vulnerabilidades descobertas eram de aplicações web (figura 4). Isso traz sérias implicações para os usuários porque eles não podem mais confiar de maneira acrítica em sites conhecidos.

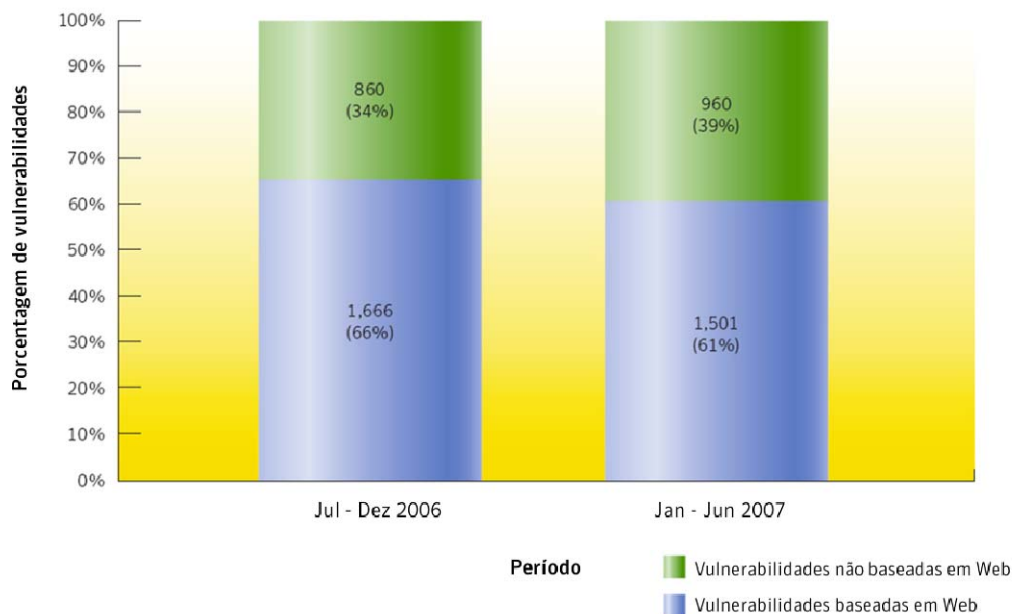


Figura 4. vulnerabilidades baseadas em aplicações Web

Fonte : Symantec Corporation

Houve também um número de exemplos onde os atacantes comprometeram web sites de confiança a fim de ficar a espreita e em busca de usuários desprevenidos. Por exemplo, muitos cavalos de Tróia estão sendo instalados através de páginas web que exploram vulnerabilidades do browser ou de plug-ins relacionados ao browser. Na primeira metade de 2007, a Symantec documentou 237 vulnerabilidades em plug-ins de browsers da web, mais de três vezes o número de vulnerabilidades de plug-ins detectadas durante o período do relatório anterior. Dois exemplos bastante visíveis que exploram esse tipo de vulnerabilidade são as famílias de cavalos de Tróia Metajuan²⁶ e Vundo²⁷, ambas detectadas pela Symantec na primeira metade de 2007. Conforme o Web browser tornou-se a aplicação padrão no mundo da Web 2.0, esses plug-ins e suas vulnerabilidades ofereceram todo um novo campo a ser explorado.

No volume X do Relatório sobre Ameaças à Segurança na Internet, a Symantec previu que tecnologias Web 2.0 apresentariam novas oportunidades a serem exploradas pelos criminosos.²⁸ Essa previsão parece ter se confirmado. Os atacantes frequentemente tirarão vantagem da confiança implícita entre a comunidade de usuários para comprometer usuários individuais ou páginas da Web, ou ainda para criar, eles próprios, páginas da Web.

Ataques contra sites confiáveis são frequentemente muito valorizados pelos criminosos porque eles podem ser usados para expor informação confidencial do usuário, tais como nomes de usuário, senhas e informação sobre contas. Tais informações poderiam então ser usadas para roubo de identidade ou fraude, ou indiretamente para acessar sites a partir dos quais podem lançar ataques posteriores, tais como hospedar sites de phishing utilizando credenciais de hospedagem de ISPs e Web comprometidos.

²⁶ http://www.symantec.com/security_response/writeup.jsp?docid=2007-030112-0714-99

²⁷ http://www.symantec.com/security_response/writeup.jsp?docid=2004-112111-3912-99

²⁸ Symantec *Internet Security Threat Report*, Volume X (September 2006):

http://eval.symantec.com/mktginfo/enterprise/white_papers/entwhitepaper_symantec_internet_security_threat_report_x_2006.en-us.pdf : p. 27

A informação obtida com um ataque de phishing bem sucedido contra um site de relacionamento social poderia ser usada para propagar códigos maliciosos para outros usuários da rede, para roubar informação de contas de outros usuários, ou para reunir endereços para envio de spam. Por exemplo, durante os primeiros seis meses de 2007, um importante site de relacionamento social estava entre as 10 marcas mais visadas por phishing.

Outro exemplo da mudança na estratégia dos atacantes é a distribuição de alguns códigos maliciosos. Tradicionalmente, códigos maliciosos eram enviados a um alvo visado, com frequência como anexos de e-mail. Porém, cada vez mais, códigos maliciosos como cavalos de Tróia são instalados pelos atacantes e induzem os usuários a visitar páginas da web que podem explorar vulnerabilidades no browser do usuário ou seus componentes. O código malicioso em si mesmo não explora diretamente quaisquer vulnerabilidades neste cenário, mas ao invés disso é instalado em um computador através da exploração de uma vulnerabilidade. Durante a primeira metade de 2007, 18% dos 1509 códigos maliciosos documentados foram instalados em computadores através deste método.²⁹ Enquanto que esse é um número mais baixo do que os 23% dos 1.318 exemplos de códigos maliciosos documentados na segunda metade de 2006, os sites visados têm o potencial de alcançar números maiores de usuários e portanto aumentando as chances de propagação em larga escala.

Convergência dos métodos de ataque

Tradicionalmente, o Relatório sobre Ameaças à Segurança na Internet tem analisado e discutido a atividade de segurança como um conjunto de atividades separadas: ataques à Internet, vulnerabilidades, códigos maliciosos, phishing, spam e outras atividades maliciosas. Enquanto que este relatório continua a manter aquela estrutura, durante os dois últimos períodos analisados, tem tornado-se cada vez mais aparente que enquanto essas ameaças eram frequentemente usadas de maneira separada no passado, os atacantes estão agora consolidando métodos de ataque diversos para criar redes globais que dão suporte a atividades maliciosas coordenadas. Isto é, a Symantec notou uma convergência de vários componentes na atividade de ataque que é devida a crescente inter-conectividade e funcionalidade cruzada de varias atividades maliciosas.

O MPack é um bom exemplo desta convergência. A Symantec classifica o MPack como código malicioso, especificamente como cavalo de Tróia. Entretanto, a fim de instalá-lo no computador de um usuário, o atacante deve primeiro gerar tráfego para os servidores MPack. Isso pode ser conseguido de diversas formas, a primeira delas é através do comprometimento de web sites legítimos, que farão com que o browser do usuário seja redirecionado quando visite aqueles sites. De maneira alternativa, o atacante pode enviar links para servidores maliciosos em mensagens de spam. Esses servidores, por sua vez, redirecionam o browser do usuário para o servidor MPack. Em alguns casos, os atacantes estabelecem domínios de “typosquatting” que direcionam os usuários aos servidores MPack.³⁰

Uma vez que o usuário é redirecionado para um servidor MPack, ele explora uma das muitas vulnerabilidades no browser da web ou de vários plug-ins do browser a fim de baixar e instalar um cavalo de Tróia no computador. Este cavalo de Tróia é o primeiro estágio de um multistaged downloader, que por sua vez baixa e instala outras ameaças no computador afetado.

²⁹ deve-se notar que o número de códigos maliciosos documentados difere do número de casos de códigos maliciosos apresentados. Exemplos de códigos maliciosos são aqueles que tenham sido analisados e registrados dentro do banco de dados sobre códigos maliciosos da Symantec.

Como o MPack, outros cavalos de Tróia exibem essa convergência de ameaças. Uma vez instalado em um computador, eles podem ser usados para visualizar informação confidencial que pode ser usada posteriormente em roubo de identidade ou fraude. Eles podem também ser usados para lançar ataques de phishing e/ou para hospedar web sites de phishing. Finalmente, eles podem ser usados como zumbis de spam.

Os Bots também exemplificam esta tendência. Eles permitem uma ampla gama de funcionalidades e a maior parte pode ser atualizada para assumir novas funções através do download de novos códigos e características. Bots também podem ser usados por atacantes externos para realizar ataques de negação de serviço contra o web site de uma organização. Além do mais, uma vez na rede da organização, eles podem ser usados para atacar os websites de outras organizações. Os bots podem ser usados por atacantes para colher informação confidencial de computadores afetados, o que pode levar ao roubo de identidade ou outras atividades fraudulentas. Eles também podem ser usados para distribuir spam e para ataques de phishing.

Conforme os atacantes têm tornado-se cada vez mais motivados por ganhos financeiros, esta convergência de atividades permitiu que eles otimizem as capacidades de um largo espectro de métodos de ataque. Isso sugere que desenvolvedores de códigos exploradores, autores de códigos maliciosos, emissores de spam e de phishing podem estar colaborando a fim de obter benefício mútuo. Isso também indica que um novo tipo de atacante versado em todos esses diferentes tipos de ataque tenha surgido, contando ainda com extrema flexibilidade em sua metodologia de ataque.

Conforme os ataques convergem e se tornam mais complexos do que antes, é importante fornecer proteção completa para computadores e redes de computadores de empresas. No passado grupos diferentes eram frequentemente responsáveis por vários aspectos da proteção da rede de uma companhia – proteção de desktop, operações de servidor e rede, grupos anti-virus, e equipes anti-spam. Agora é imperativo que esses grupos trabalhem juntos e compartilhem informação já que uma única ameaça pode afetar todos eles.

Destaques do Volume XII do Relatório sobre Ameaças à Segurança na Internet Symantec

A seção seguinte oferecerá um breve resumo das tendências de segurança que a Symantec observou no Volume XII do Relatório sobre Ameaças à Segurança na Internet. Este resumo inclui todos os parâmetros incluídos no relatório principal.

Destaques nas tendências de ataques globais

- Os Estados Unidos foram o país mais visado pelos ataques de negação de serviço (DoS), respondendo por 61% do total mundial na primeira metade de 2007.
- Os Estados Unidos foi o principal país de origem dos ataques nos primeiros seis meses de 2007, respondendo por 25% da atividade de ataque mundial.
- Durante esse período os EUA, respondeu por 30% de toda a atividade maliciosa durante o período, mais do que qualquer outro país.
- Israel foi o país com a maior atividade maliciosa por usuário de Internet nos primeiros seis meses de 2007, seguido por Canadá e Estados Unidos.
- 4% de toda a atividade maliciosa detectada durante os primeiros seis meses de 2007 teve origem em

³⁰ Typosquatting é a prática de registrar nomes de domínios que sejam parecidos com o de um domínio legítimo que pode incluir um erro comum de ortografia. Por exemplo, um domínio de typosquatting para google.com pode ser gogle.com

espaços IP registrados para empresas da lista Fortune 100.

- O setor de educação foi responsável por 30% das brechas em dados que poderiam levar a roubo de identidade durante este período, mais do que qualquer outro setor.
- Roubo ou perda de computador ou outro meio de armazenagem de dados contribuiu com 46% de todas as brechas de dados que poderiam levar a roubo de identidade durante este período.
- Os Estados Unidos foi o principal país em numero de servidores informais, figurando com 64% do total de servidores informais conhecidos pela Symantec.
- Cartões de crédito foram a mercadoria mais frequentemente posta à venda em servidores informais detectados pela Symantec, respondendo por 22% de todos os itens.
- 85% dos cartões de crédito postos a venda em servidores informais detectados pela Symantec haviam sido emitidos por bancos nos Estados Unidos.
- A Symantec observou uma média de 52.771 computadores infectados por bot em atividade por dia na primeira metade de 2007, uma redução de 17% em relação ao período anterior.
- A China teve 29% do total mundial de computadores infectados por bot, mais do que qualquer outro país.
- Os Estados Unidos teve o mais alto número de servidores bot de comando e controle, respondendo por 43% do total mundial.
- Beijing foi a cidade com o maior número de computadores infectados por bot, respondendo por 7% do total mundial.
- O tempo de vida médio de um computador infectado por bot durante os seis primeiros meses de 2007 foi de 4 dias, contra o tempo médio de 3 dias registrado na segunda metade de 2006.
- Usuários domésticos foram o setor mais visado, respondendo por 95% de todos os ataques efetuados.

Destaques nas tendências de vulnerabilidade global

- A Symantec documentou 2.461 vulnerabilidades na primeira metade de 2007, 3% menos do que na segunda metade de 2006.
- A Symantec classificou 9% de todas as vulnerabilidades descobertas durante este período como de alta severidade, 51% de média severidade e 40 % como sendo de baixa severidade. Na segunda metade de 2006, 4% das vulnerabilidades recém descobertas eram de alta severidade, 69% eram de média severidade e 27% de baixa severidade.
- 61% das vulnerabilidades descobertas neste período afetaram aplicações Web, contra 66% no último semestre de 2006.
- 62% das vulnerabilidades documentadas durante este período eram facilmente exploráveis. Isso é uma diminuição em relação aos 79% do período coberto pelo relatório anterior.
- Na primeira metade de 2007, todos os sistemas operacionais exceto Hewlett Packard® HP-UX® tiveram tempos de desenvolvimento médio de patches menor na segunda metade de 2006.
- Hewlett-Packard HP-UX teve um tempo médio de desenvolvimento de patch de 112 dias na primeira metade de 2007, a mais alta dentre todos os sistemas operacionais. A Sun teve o tempo médio de desenvolvimento de patch mais alto na segunda metade de 2006, com 145 dias.
- A janela média de exposição a vulnerabilidades afetando vendedores corporativos foi de 55 dias. Isso representa um aumento em comparação a media de 47 dias na segunda metade de 2006.
- A Symantec documentou 39 vulnerabilidades no Microsoft® Internet Explorer, 34 no Mozilla, 25 no

Safari™ da Apple®, e 7 no Opera. Na segunda metade de 2006, 54 vulnerabilidades foram descobertas para o Internet Explorer, 40 para o Mozilla, 4 para o Safari da Apple, e 4 para o Opera.

- O Safari da Apple teve uma janela media de exposição de 3 dias na primeira metade de 2007, a mais curta dentre todos os browsers analisados no período. O Mozilla teve a mais curta janela media de exposição na segunda metade de 2006, dois dias.
- A Symantec documentou 6 vulnerabilidades zero-day na primeira metade de 2007, menos do que as 12 reportadas na segunda metade de 2006.
- 97 vulnerabilidades foram documentadas em Oracle®, mais do que qualquer outro banco de dados durante a primeira metade de 2007. Oracle também teve o maior numero de vulnerabilidades de banco de dados na segunda metade de 2006, com 168.
- Havia 90 vulnerabilidades corporativas para as quais não havia ainda patch disponível na primeira metade de 2007, o que menos do que as 94 documentadas na segunda metade de 2006. A Microsoft teve o maior numero de vulnerabilidades para as quais não havia patch dentre todos os produtores de softwares corporativos durante ambos os períodos.
- Na primeira metade de 2007, a Symantec documentou 237 vulnerabilidades em plug-ins de Web browsers. Isso é um aumento significativo em comparação a 74 na segunda metade de 2006, e 34 na primeira metade de 2006.
- Durante a primeira metade de 2007, 89% das vulnerabilidades de plug-ins descobertas afetaram componentes ActiveX® para Internet Explorer. Componentes ActiveX responderam por 58% das vulnerabilidades de plug-ins na segunda metade de half of 2006.
- A Symantec concluiu que mais de 50% das vulnerabilidades de media e alta severidade que receberam patches dos fabricantes afetaram Web browsers ou tiveram outros vetores de ataque do lado cliente durante este e durante o período de relatório anterior. A Apple foi a única exceção, com 49% das vulnerabilidades examinadas na primeira metade de 2007 afetando browsers ou tendo vetores de ataque do lado cliente.

Destaques nas tendências globais de códigos maliciosos

- Dentre as dez mais importantes famílias de novos códigos maliciosos detectados na primeira metade de 2007, 4 eram cavalos de Tróia, três eram vírus, 1 era worm, e 2 eram worms com um componente de vírus.
- Na primeira metade de 2007, 212,101 novos códigos maliciosos foram reportados à Symantec. Isso representa um aumento de 185 % sobre a segunda metade de 2006.
- Durante a primeira metade de 2007, cavalos de Tróia responderam por 54% do volume dos principais 50 relatos de códigos maliciosos, um aumento em relação aos 45% reportados nos seis últimos meses de 2006.
- Quando considerados quanto a potenciais infecções, os cavalos de Tróia responderam por 73% das 50 principais amostras de códigos maliciosos, mais do que os 60 % do período anterior.
- Durante este período 43% das infecções por worms foram reportadas na região da Europa, Oriente Médio e África.
- A América do Norte respondeu por 44% dos cavalos de Tróia reportados neste período.
- Ameaças a informações confidenciais totalizaram 65% das 50 principais amostras de códigos maliciosos com maior potencial de infecção reportados à Symantec.

- Ameaças com capacidade de Keystroke-logging perfizeram 88% das ameaças a informações confidenciais durante o período, tanto quanto ameaças com capacidades de acesso remoto, tais como back doors. Isso representa um aumento a partir de 76% e 87% respectivamente, em relação ao período anterior.
- 46% dos códigos maliciosos propagados utilizaram-se de SMTP, tornando-o o mecanismo de propagação mais comum.
- Durante a primeira metade de 2007, 18% dos 1,509 códigos maliciosos documentados exploraram vulnerabilidades.
- 35% dos computadores infectados reportaram mais de uma infecção na primeira metade de 2007.
- Oito dentre os mais freqüentes staged downloaders encontrados no período eram cavalos de Tróia e dois eram worms.
- Sete dentre os 10 componentes mais frequentemente descarregados eram cavalos de Tróia e 3 eram back doors.
- Códigos maliciosos que visam jogos on-line games responderam por 5% dos 50 codigos maliciosos mais importantes de acordo com potencial de infecção.
- Lineage e World of Warcraft foram os 2 jogos on line mais frequentemente visados na primeira metade de 2007.

Destaques no Phishing global

- A Symantec Probe Network detectou um total de 196.860 mensagens exclusivas de phishing, um aumento de 18% em relação aos últimos seis meses de 2006. Isso corresponde a uma media de 1.088 mensagens exclusivas de phishing por dia para a primeira metade de 2007.
- A Symantec bloqueou mais de 2.3 bilhões de mensagens de phishing, o que representa um aumento de 53% sobre a última metade de 2006. Isso significa que a Symantec bloqueou uma media de aproximadamente 12.5 milhões de e-mails de phishing por dia durante os primeiros meses de 2007.
- organizações no setor de serviços financeiros responderam por 79% das marcas exclusivas que foram usadas em ataques de phishing durante este período.
- as marcas de organizações do setor de serviços financeiros foram imitadas por 72% de todos os web sites de phishing.
- 59% de todos os websites de phishing conhecidos eram localizados nos Estados Unidos , uma proporção muito maior do que a de qualquer outro país.
- Três kits de ferramentas de phishing foram responsáveis por 42% de todos os ataques de phishing observados pela Symantec na primeira metade de 2007.
- 86% de todos os web sites de phishing estavam hospedados em apenas 30% dos endereços IP conhecidos como servidores de phishing.

Destaques no spam global

- Entre 1º de Janeiro e 30 de junho de 2007, o spam correspondeu a 61% de todo o trafego de e-mail monitorado. Isso representa um ligeiro aumento em relação aos últimos seis meses de 2006, quando 59% do e-mail foi classificado como spam.
- 60% de todo o spam detectado durante este período foi composto em Inglês, menos do que os 65% encontrado no período equivalente ao relatório anterior.

- Na primeira metade de 2007, 0.43% de todo o e-mail considerado como spam continha códigos maliciosos, comparado com 0,68% na segunda metade de 2006. Isso significa que um de cada 233 mensagens de spam bloqueadas pelo Symantec Brightmail AntiSpam™ durante o período do relatório atual continha códigos maliciosos.
- Spam relacionado a produtos comerciais correspondeu a 22% de todo o spam durante este período, o número mais alto de qualquer categoria.
- Durante os seis primeiros meses de 2007, 47% de todo o spam detectado mundialmente foi originado nos Estados Unidos comparado com 44% no período anterior.
- Nos seis primeiros meses de 2007, 10% de todos os zumbis de spam no mundo eram localizados nos Estados Unidos, mais do que em qualquer outro país.
- Na primeira metade de 2007, 27% de todo o spam bloqueado pela Symantec era spam de imagem.

Resumo Executivo do Relatório de Ameaças à Segurança na Internet para o setor Governamental

A próxima seção oferecerá um resumo breve da atividade de segurança que a Symantec observou nos setores de governo e infra-estrutura durante a primeira metade de 2007. Este resumo inclui todos os parâmetros que estão incluídos no Relatório de Ameaças à Segurança na Internet para o Governo.

Destaques das tendências de ataques ao setor governamental

- Entre 1º de Janeiro e 30 de junho de 2007, os Estados Unidos foram o principal país em atividade maliciosa, respondendo por 30% da atividade detectada mundialmente.
- Israel teve a maior atividade maliciosa por usuário de Internet, seguido por Canadá e Estados Unidos.
- Nos primeiros seis meses de 2007, 90 % de toda a atividade maliciosa originária de setores de infra-estrutura crítica originaram-se de setores de telecomunicações.
- Durante o período deste relatório, o setor governamental correspondeu a 26% das brechas de dados que poderiam levar a roubo de identidade, fazendo com que ele ficasse como o segundo maior setor para esse quesito.
- A causa primária de brechas de dados que poderiam facilitar o roubo de identidade foi o roubo ou perda de um computador ou outro meio para armazenagem ou transmissão de dados, tais como uma chave USB ou uma mídia de back-up.
- A atividade de Hackers foi responsável por 73% das identidades expostas durante o período.
- Os Estados Unidos foi o alvo da maior parte dos ataques de negação de serviço, respondendo por 61% de todos os ataques durante este período.
- Entre 1º de Janeiro e 30 de junho de 2007, a Symantec observou uma média de 52.771 computadores ativos infectados por bots por dia, uma queda de 17% em relação ao período do relatório anterior.
- O tempo de vida médio de um computador infectado por bot foi de 4 dias, um aumento em relação aos 3 dias da segunda metade de 2006.
- A China teve o mais alto número de computadores infectados por bot durante a primeira metade de 2007, correspondendo a 29% do total mundial.
- Os Estados Unidos tiveram o maior número de servidores de comando e controle do mundo,

respondendo por 43% do total mundial.

- Os Estados Unidos foi o principal país como origem de ataques, ficando com 25% da atividade mundial de ataques, um decréscimo em relação aos 33% obtidos durante a última metade de 2006.
- O principal país de origem para os ataques detectados por sensores colocados no setor governamental na primeira metade de 2007 foram os Estados Unidos, respondendo por 19% do total.
- A maioria dos ataques captados por todos os sensores do setor governamental e de infra-estrutura crítica nos primeiros seis meses de 2007 foram ataques baseados em SMTP, respondendo por 36% dos principais ataques.

Destaques nas tendências de vulnerabilidade para o setor governamental

- Dos cinco sistemas operacionais rastreados nos primeiros seis meses de 2007, a Microsoft teve o menor tempo médio de desenvolvimento de patch com 18 dias, baseado em um conjunto de amostras de 38 vulnerabilidades sanadas.
- A Symantec documentou seis vulnerabilidades zero-day durante este período, menos do que as 12 vulnerabilidades zero-day encontradas na segunda metade de 2006.
- Na primeira metade de 2007, a Symantec documentou 90 vulnerabilidades corporativas não cobertas por patches de segurança que foram publicadas durante este período.

Destaques de tendências de códigos maliciosos para o setor governamental

- Nos primeiros seis meses de 2007, ameaças a informação confidencial correspondeu a 65% de infecções em potencial para as 50 principais amostras de códigos maliciosos. Isso representa um aumento em relação aos 53% de infecções em potencial na segunda metade de 2006.
- 88% das ameaças à informação confidencial tinham capacidades de acesso remoto, um pouco acima dos 87% detectados no período anterior.
- 88% das ameaças à informação confidencial tinham capacidades de keystroke-logging, acima dos 76% detectados na segunda metade de 2006.
- Na segunda metade de 2007, 46% dos códigos maliciosos propagados o fizeram através de anexos de e-mail.
- No período atual, os Estados Unidos foram o país com mais alto número de infecções com múltiplos códigos maliciosos no mundo, seguido por China e Japão.
- Entre Janeiro e junho de 2007, 44% dos cavalos de Tróia foram reportados da América do Norte, enquanto que 37% foram reportados da região da Europa, Oriente Médio e África.
- A região da Europa, Oriente Médio e África respondeu por 43% de potenciais infecções causadas por worms. Isso foi seguido pela região da Ásia-Pacífico e Japão, que respondeu por 29% das potenciais infecções por worms.
- A região da Europa, Oriente Médio e África respondeu por 45% das infecções potenciais por vírus deste período, seguida pela região da Ásia-Pacífico e Japão, que respondeu por 27% das infecções por vírus no mundo.
- A região da Europa, Oriente Médio e África respondeu por 40% de todas as infecções potenciais por back doors no mundo, e a América do Norte respondeu por 33%.

Destaques nas tendências de Phishing para o setor governamental

- 79% das organizações cujas marcas foram usadas em ataques de phishing nos primeiros seis meses de 2007 foram no setor de serviços financeiros, abaixo dos 84% na segunda metade de 2006.
- O setor de serviços financeiros também respondeu por 72% do volume de todos os web sites de phishing, ficando acima dos 64% do período anterior.
- Na primeira metade de 2007, 59% de todos os sites de phishing conhecidos eram localizados nos Estados Unidos, comparado aos 46% dos seis meses anteriores.
- Durante os primeiros seis meses de 2007, 23% dos domínios exclusivos do setor governamental usados para hospedar web sites de phishing eram localizados na Tailândia.

Resumo Executivo do Relatório de Ameaças à Segurança na Internet para a Região da Europa, Oriente Médio e África (EMEA)

A seção seguinte oferecerá um breve resumo da atividade de segurança observada pela Symantec durante a primeira metade de 2007 na região da Europa, Oriente Médio e África. Este resumo inclui todos os parâmetros que se encontram incluídos no Relatório Sobre Ameaças à Segurança na Internet na Região da Europa, Oriente Médio e África.

Destaques nas tendências de ataques na região da EMEA

- Durante os seis primeiros meses de 2007, os Estados Unidos foram o país de origem da maioria dos ataques contra computadores localizados na EMEA, respondendo por 35% dos ataques detectados por sensores na região.
- Durante os seis primeiros meses de 2007, o Reino Unido foi o país da EMEA mais frequentemente visado por ataques de negação de serviço, respondendo por 46% dos ataques na região durante este período.
- Entre 1º de Janeiro e 30 de junho de 2007, a Symantec observou uma média de 18,616 computadores ativos infectados por bot por dia na região EMEA, um número mais baixo do que os 21,707 vistos durante o período do relatório anterior. A Symantec também detectou 52,771 bots ativos por dia no mundo inteiro, então a região da EMEA respondeu por 41% dos bots ativos em um dia médio.
- Entre 1º de Janeiro e 30 de junho de 2007, a Alemanha teve o mais alto número de computadores infectados por bots na região da EMEA, respondendo por 23% do total. Isso é um aumento em relação aos 16% detectados na segunda metade de 2006, quando a Alemanha foi classificada em segundo lugar na região da EMEA por computadores infectados por bot.
- Madrid na Espanha foi a cidade da EMEA com o mais alto número de computadores infectados por bot durante os primeiros seis meses de 2007, permanecendo como estava no período do relatório passado.
- O setor de usuários domésticos foi de longe o mais visado na região da EMEA, ficando com 99.4% de todos os ataques visados, o que não apresentou mudança desde o período anterior.
- Nos primeiros seis meses de 2007, a Alemanha respondeu por 19% da atividade maliciosa na região da EMEA, a maior dentre quaisquer outros países. Essa foi a mesma porcentagem e posição da segunda metade de 2006.
- Israel teve a maior atividade maliciosa por usuário de Internet na região da EMEA, seguido por Polônia e Espanha.

Destaques em códigos maliciosos na região da EMEA

- Durante os primeiros seis meses de 2007, cavalos de Tróia foram o tipo de código malicioso mais comum na EMEA, respondendo por 68% dos relatos de códigos maliciosos recebidos da região.
- O Reino Unido foi o principal país da região EMEA em infecções potenciais por back doors e Cavalos de Tróia.
- A Índia foi o principal país da região da EMEA para infecções potenciais de vírus e worms.
- A principal amostra de códigos maliciosos na região da EMEA foi o worm de e-mail em massa Netsky.P, que foi o segundo tipo de código malicioso mais comum na segunda metade de 2006.
- A família de códigos maliciosos que mais prevaleceu na região da EMEA durante os primeiros seis meses de 2007 foi o Metajuan Trojan, que foi a terceira mais frequentemente reportada família de códigos maliciosos do mundo durante esse período.
- Ameaças a informação confidencial corresponderam a 61% do volume dos 50 principais códigos maliciosos causadores de potenciais infecções a partir da região da EMEA, menos do que a porcentagem mundial de 65%.
- Ameaças que permitem acesso remoto, tais como back doors, totalizaram 87% das ameaças a informação confidencial por volume de relatórios.
- Arquivos anexados a e-mails foram usados por 49% das amostras propagandas de códigos maliciosos detectados na região da EMEA durante este período, fazendo deles o mecanismo de propagação mais comum na região. Esse método também respondeu por 46% do volume das amostras em propagação no mundo todo.

Destaques das tendências de phishing na região da EMEA

- Durante os primeiros seis meses de 2007, a Alemanha teve a mais alta porcentagem de web sites de phishing na EMEA com 22% do total regional. Esse foi o segundo mais alto país no mundo para web sites de phishing depois dos Estados Unidos.
- Karlsruhe, na Alemanha foi a cidade com maior número de sites de phishing na região da EMEA nos primeiros seis meses de 2007, como havia sido no período anterior.

Resumo Executivo do Relatório de Ameaças à Segurança na Internet para a região da Ásia - Pacífica e Japão (APJ)

A seção seguinte oferecerá um breve resumo da atividade de segurança que a Symantec observou durante a primeira metade de 2007 na região da Ásia-Pacífico e Japão. Este resumo inclui todos os parâmetros que estão incluídos no Relatório sobre Ameaças à Segurança na Internet para a região da Ásia-Pacífico e Japão.

Destaques nas tendências de ataques para a região da APJ

- Os Estados Unidos foram o país de origem da maioria dos ataques contra computadores localizados na região da APJ, respondendo por 29% dos ataques detectados.
- A China foi visada por 74% dos ataques a região da APJ durante este período, apresentando, portanto um aumento em relação aos 63% vistos durante o período anterior.
- A Symantec observou uma média de 15.447 diferentes computadores infectados por bots em

atividade na região da APJ por dia, o que equivale a 29% do total mundial de 52.771.

- A China teve o maior número de computadores infectados por bots na região da APJ, respondendo por 78% do total, mais do que os 71% detectados na segunda metade de 2006.
- Beijing foi a cidade com o maior número de computadores infectados por bot durante os primeiros seis meses de 2007, continuando na mesma posição em que esteve durante o período anterior.
- O usuário doméstico recebeu 97% de todos os ataques visados, menos do que os 98% na segunda metade de 2006.
- A China respondeu por 42% da atividade maliciosa na região da APJ, a maior dentre todos os países, mais do que os 39% do período anterior.
- O Sri Lanka foi o país colocado mais alto no ranking de países com maior atividade maliciosa por usuário de Internet, seguido por Bangladesh e Taiwan.

Destaques nas tendências de códigos maliciosos na região da APJ

- Cavalos de Tróia responderam por 51% do volume de relatórios de códigos maliciosos vindos da região APJ. Durante o mesmo período, eles totalizaram 73% do volume de relatórios de códigos maliciosos no mundo inteiro.
- A China foi o principal país da região APJ em tipos de códigos maliciosos com exceção de worms, para os quais o Japão apareceu em primeiro lugar.
- A amostra de código malicioso reportado com mais frequência na região da APJ foi o Gampass Trojan. 84% das potenciais infecções mundiais por Gampass tiveram origem nesta região.
- A família de novos códigos maliciosos mais reportada na região da APJ durante este período foi o worm Fubalca.
- Ameaças à informação confidencial totalizou 57% das infecções potenciais pelos 50 principais amostras de códigos maliciosos na região da APJ.
- De todas as ameaças a informação confidencial na região da APJ, 79% poderiam ser usadas para exportar dados do usuário e 78% tinham um componente de Keystroke-logging.
- SMTP foi o mecanismo de propagação mais comum na região da APJ, tendo sido usado por 37% dos códigos maliciosos propagados durante este período.

Destaques nas tendências de phishing para a região da APJ

- O Japão foi o país onde se concentrou a mais alta porcentagem de web sites de phishing na região da APJ, mas apenas como o 8º número mais alto no mundo.
- Taipei foi a cidade com o maior número de websites de phishing na região da APJ nos primeiros seis meses de 2007, permanecendo igual ao período anterior.

De olho no futuro

Esta seção do Relatório de Ameaças à Segurança na Internet discutirá tendências emergentes e assuntos que a Symantec acredita tornar-se-ão proeminentes no período dos próximos seis a vinte e quatro meses. Estas previsões são baseadas em pesquisa emergente que a Symantec coletou durante o período do relatório atual e são, por natureza, especulativas. Ao discutir potenciais tendências futuras, a Symantec

espera dar às organizações e aos usuários finais uma oportunidade de preparar-se para questões de segurança complexas e de rápido desenvolvimento. Esta seção discutirá potenciais assuntos de segurança associados como o seguinte:

- Códigos maliciosos e mundos virtuais
- Processos de evasão automatizados — esconde-esconde para a geração segurança
- Ameaças da Web avançadas — origens da lavagem através da Web
- Diversificação no uso de bots

Códigos maliciosos e mundos virtuais

Um mundo virtual persistente (PVW) é um ambiente on-line simulado no qual os usuários podem criar personagens conhecidas como avatares. Esses avatares podem interagir entre si em um ambiente de realidade simulada, 24 horas por dia, sete dias por semana. O Second Life é provavelmente o exemplo mais conhecido de um PVW.

Mundos virtuais frequentemente servem como ambientes nos quais numerosos usuários interagem em jogos on-line para diversos jogadores (MMOGs). Exemplos populares de MMOGs incluem World of Warcraft e Lineage, ambos permitindo que milhares de jogadores possam interagir on-line ao mesmo tempo. PVWs e MMOGs são extremamente populares, e tem sido amplamente adotados e áreas como a China e a Coréia do Sul. A Symantec acredita que conforme o uso desses ambientes virtuais se expande, um número de preocupações de segurança surgirão.

Uma razão simples para isso é que a audiência de PVWs e MMOGs são usuários precoces (early adopters), pessoas que freqüentemente já usam computadores. Conforme MMOGs tornam-se mais difundidos e jogados por novos usuários de computadores, as técnicas de ataques que visam estes ambientes provavelmente se tornara mais eficiente. A população geral (isto é, jogadores casuais) é provavelmente uma audiência que os atacantes começarão a visar mais.

Muitos PVWs e MMOGs permitem que os jogadores possam realizar transações com dinheiro real (RMT) em mundos virtuais. Os jogadores podem usar cartões de crédito ou outros meios de pagamento para comprar créditos virtuais e então trocar aqueles créditos com jogadores em outros países, onde eles podem ser retirados na moeda local. Essas RMTs produzem um sistema monetário real. Há até mesmo trocas virtuais de moeda entre mundos virtuais ou entre jogos diferentes.

Estes mercados (também chamados de economias secundárias) são atualmente não-regulamentados e são ainda muito pequenos para atrair seriamente a atenção da lei e de regulamentadores de mercados. A Symantec acredita que essas características poderiam permitir que criminosos façam uso delas para atividades criminosas. Por exemplo, por causa da anonimidade oferecida por PVWs, onde todas as identidades são virtuais, criminosos podem ser capazes de lavar dinheiro através do uso de RMTs.

Para facilitar isso, uma empreitada criminosa poderia abrir muitos milhares de contas MMOG. Cada conta poderia ser usada para trocas com outros jogadores, na compra ou venda de bens dentro do jogo; utilizando para isso os fundos que seriam em última instância retirados das contas em questão. Já que milhares de contas podem ser usados em milhares de transações, cada uma com pequenos lucros ou perdas, seria difícil rastrear a fonte real dos fundos quando eles forem retirados. Essas transações podem ser feitas no mundo inteiro sem o controle que normalmente acompanha operações monetárias internacionais. De fato, em fevereiro de 2007, o banco central da China e ministros das finanças determinaram que as empresas parassem de trocar moedas QQ e moedas virtuais, presumivelmente para burlar a troca não regulamentada

de moedas.³¹

Além do mais, Sparter criou um sistema de troca de moedas entre jogos chamado Gamer2Gamer que permite que os jogadores enviem suas mercadorias e moedas MMOG.³² Atualmente o World of Warcraft da Blizzard Entertainment, Lord of the Rings Online da Turbine, o EverQuest II da Sony Online Entertainment e o CCP da EVE Online tem suporte para esse recurso. Disponibilidade dessas plataformas encorajará o uso de PVWs e MMOGs por parte de atacantes como veículos de lavagem de dinheiro.

A Symantec também acredita que os atacantes usarão PVWs e MMOGs para persuadir as vítimas a instalar softwares maliciosos sob a argumentação de que o software melhora a funcionalidade no mundo virtual. Por exemplo, mundos virtuais abraçaram o conceito de bots de script que servem, entretêm e protegem avatares dentro do mundo virtual. Isso poderia dar aos atacantes uma oportunidade para comprometer o ambiente em si mesmo.

Embora a maioria dos MMOGs sejam projetados para ser jogados por jogadores, ferramentas automáticas podem ser usadas para melhorar os recursos de jogo e evitar algumas atividades repetitivas e tediosas. O download e uso dessas ferramentas apresentam uma oportunidade para que os atacantes incorporem programas maliciosos tais como keystroke loggers e ladrões de senhas e informação, os quais o usuário pode inadvertidamente instalar em seu computador. A Symantec já observou códigos maliciosos que tentam roubar informação e senhas de jogadores, tais como.³³ A Symantec espera que conforme kits de ferramentas próprias de um jogo tornem-se mais difundidas e usadas por mais jogadores, os atacantes alterarão seus esforços para infectar extensões do jogo.

Jogadores MMOG e residentes de comunidades virtuais podem também ser visados por phishers e spammers. Por exemplo, usuários desses ambientes podem receber e-mails que alegam ser dos administradores do jogo que direcionam os usuários para web sites falsos que são projetados para capturar informação de contas, tais como o nome de usuário e senha. O phisher terá então acesso a conta do jogador, a partir da qual eles podem distribuir os bens do jogador entre outros avatares ou vender a conta a outro jogador. Apesar do risco, a tentação de comprar uma conta estabelecida, com um nível de jogo alto e posses estabelecidas por um relativo desconto (comparado com gastar milhares de horas jogando o jogo, ganhando aquele nível e acumulando posses similares) continua a atrair compradores.

Similar ao phishing, a Symantec também espera ver um aumento no montante de spam que é enviado sobre os canais internos dos jogos. Emissores de spam tentarão conseguir nomes de personagens em web sites que mostram as divisões de jogo, ou eles podem usar scripts automatizados para coletar nomes de jogadores. Uma vez que spam chegue por meio das comunicações internas do jogo – o pode consistir de clientes de instant messaging que são construídos dentro do ambiente do jogo em si mesmo – poderia ser usado para propagar ataques de phishing ou códigos maliciosos, ou para direcionar os usuários para sites maliciosos.

³¹ http://online.wsj.com/public/article/SB117519670114653518-dn8gNFq5f7FniF4G8iQ_gbzDKug_20080328.html

³² <http://www.shacknews.com/onearticle.x/47408>

³³ http://www.symantec.com/security_response/writeup.jsp?docid=2005-073115-1710-99

Processos de evasão automática — esconde-esconde para a geração segurança

Dispositivos anti-vírus não são solidamente baseados em comportamento. Alguns detectam arquivos maliciosos usando assinaturas estáticas, o que simplesmente envolve a busca por um string exclusivo em um arquivo particular. Outros usam análise dinâmica, que requer a execução de códigos potencialmente maliciosos em um ambiente controlado. Para desenvolver essas assinaturas, fabricantes de antivírus devem adquirir amostras de códigos maliciosos através de meios tais como envios de usuários, chamarizes ou zoológicos.³⁴ as amostras devem então serem analisadas, após cada assinatura ser produzida e empregada pelos usuários.

Quanto mais tempo um novo código permanecer não detectado, maior será a probabilidade de ele se propagar com sucesso. Conforme escritores de códigos maliciosos põem mais esforço em suas criações, a necessidade para fugir da detecção aumenta. Como resultado, eles desenvolveram diversos mecanismos de evasão.

Historicamente, polimorfismo³⁵ e metamorfismo³⁶ tanto quanto packers,³⁷ têm sido usados para evadir-se de detecção. Desse modo aumentando o tempo de vida de códigos maliciosos. Entretanto, avanços na detecção de ameaças polimórficas e metamórficas e na abertura de códigos maliciosos permitiram que fabricantes de anti-vírus produzam assinaturas que são capazes de captar a maior parte das variantes. Autores de códigos maliciosos foram então forçados a adotar novas técnicas.

Algumas das novas técnicas são centradas no ponto de distribuição o ponto onde o código malicioso é hospedado, tais como um servidor da web. Com o considerável declínio de worms baseados na web nos últimos anos (como é discutido na seção “Tendências de Códigos Maliciosos” deste relatório), os códigos maliciosos atuais frequentemente dependem da exploração de vulnerabilidades do lado cliente. Essas explorações frequentemente usam o modelo de staged downloader no qual um cavalo de Tróia inicial é instalado na máquina e então baixa a versão mais atualizada de um código malicioso de um ponto de distribuição.

A Symantec observou autores de códigos maliciosos empregando várias técnicas para proteger os servidores que são usados como pontos de distribuição. O mais básico deles é configurar um servidor de distribuição para servir apenas uma cópia de código malicioso por endereço IP, após o que ele distribui apenas um executável benigno. O propósito disto é burlar a detecção e a aquisição por companhias de segurança que necessitam de amostras do cavalo de Tróia original a fim de produzir assinaturas. Este atraso na obtenção de amostras pelas empresas de segurança aumenta as possibilidades de que os códigos maliciosos possam espalhar-se ainda mais antes da detecção.

Isso poderia trazer duas conseqüências. De um lado os computadores por trás de um Web-proxy ou de um mecanismo de translação de endereço de rede são menos propensos a tornarem-se infectados já que todos

³⁴ Códigos maliciosos que são desenvolvidos em um “zoológico” são desenvolvidos no ambiente controlado de um laboratório.

³⁵ Um vírus polimórfico é um que pode mudar seus padrões de bytes quando ele se reproduz, portanto evitando detecção por técnicas de escaneamento de um único string. Em essência, vírus polimórficos fazem mudanças em seus códigos para evitar detecção

³⁶ A evolução de códigos metamórficos descreve um método usado por escritores de códigos maliciosos que permite que um pedaço de código malicioso mude a si próprio de maneira autônoma.

³⁷ Utilitários Run-time também conhecidos como run-time packers, são tradicionalmente usados para tornar os arquivos menores. Escritores de arquivos maliciosos utilizam-nos para tornar a detecção de vírus mais difícil.

os computadores por trás de um desses dispositivos compartilham um único endereço IP. Por outro lado, um pesquisador de segurança em computadores ou analista de códigos maliciosos tentando investigar a infecção terá problema em conseguir uma amostra. Essa dificuldade ocorre porque a mesma técnica poderia ser usada para bloquear deliberadamente endereços IP registrados para certas organizações tais como fabricantes de antivírus, consultorias de segurança ou equipes de resposta a emergências com computadores. Esse fenômeno ocorreu recentemente durante incidentes com o MPack Trojan.³⁸ distribuidores de códigos maliciosos podem conseguir esses objetivos através da inclusão de endereços IP conhecidos em listas negras ou dependendo de dados WHOIS e realizando uma busca de teclado.⁴² A Symantec espera que a prevalência desta técnica de defesa seja mais amplamente utilizada no futuro graças ao sucesso documentado in exemplos onde ela foi usada anteriormente.

Outra técnica mais preocupante é conhecida como Morfismo X. Emprestada de uma idéia originalmente apresentada pela IBM, o conceito é simples: o ponto de distribuição pode enviar uma copia diferente de um código malicioso para cada visitante. Neste cenário, o código malicioso não mais tem de carregar seu próprio mecanismo metamórfico ou polimórfico. Ao invés disso, o servidor retém o mecanismo. Como esta abordagem, os métodos metamórficos ou polimórficos que são usados para mudar instancia são ocultos, tornando assim difícil produzir assinaturas que atuem confiavelmente em todas as variantes. Outra opção disponível para o distribuidor de códigos maliciosos é que o site remoto pode hospedar uma copia do código fonte original de modo que qualquer morfismo x possa ocorrer em linguagem de programação de alto nível antes de compilação, depois do que otimização de compilador pode ser usada para ofuscar a amostra.

Ameaças da Web avançadas — origens da lavagem através da Web

Conforme um número de serviços são disponíveis na web e que browsers continuam a convergir em um padrão de interpretação para linguagens de script tais como JavaScript, a Symantec espera que o número de ameaças baseadas na web continuem a crescer. Uma classe interessante de ameaças inclui aquelas que ludibriam a mesma política de origem (origin policy – SOP) nos browsers da web.³⁹

Um conceito que se empresta a burla de SOP é a mistura (mash-up). Mash-ups envolvem um serviço na web que coleta dados de outros serviços web e então agrega aqueles dados em uma nova vista. Se os dados coletados de duas origens separadas é “misturada” através de um serviço web apropriado, então o browser do usuário recebe os dois pedaços de dados através do mesmo website. Como resultado, eles parecem ter o mesmo origem, mesmo quando eles podem originar-se de duas fontes diferentes. Desse modo, códigos em JavaScript de uma das origens pode obter e modificar propriedades de dados obtidos através da segunda origem apos os dois pedaços de dados terem sido misturados.

Funcionalidades similares podem também ser fornecidas por proxies web não transparentes, como Google Translate. Esses proxies geralmente atuam como um canal que afunila qualquer conteúdo que um usuário deseje. Porque o conteúdo é afunilado, do ponto de vista do browser, o conteúdo aparece como se tivesse sido originado de um proxy, quando ele pode ter sido originado de outro lugar. Esta distinção é importante ja que ela pode levantar restrições associadas com o SOP.

Por exemplo, Jikto é uma ferramenta que alavanca tais proxies para escanear sites e encontrar vulnerabilidades web.⁴⁰ O site que esta sendo escaneado e o site que contem o código de escaneamento são

³⁸ http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2007-052712-1531-99 42 dados WHOIS armazenam o nome da pessoa ou empresa que registra um dominio e possui o espaço de um endereço IP.

³⁹ The same origin policy dictates that a document or script loaded from one origin (defined with respect to the domain, protocol, and port number) cannot access or modify a document obtained from a different origin. Note that a document or script from one origin can issue a request for a document or script from another origin; however, the first document or script cannot actually read the contents of the other document or script.

⁴⁰ http://news.com.com/2100-1002_3-6169034.html

ambos carregados através do mesmo serviço de proxy. Assim, do ponto de vista do web browser, eles parecem ter a mesma origem, embora as verdadeiras origens sejam provavelmente diferentes. Como resultado o código de escaneamento pode fazer pedidos para ler as respostas do site que está sendo escaneado sem que sofra restrições pelo SOP.

Jikto é escrito inteiramente em JavaScript então ele pode rodar no browser do usuário. Qualquer usuário que visite a página contendo a fonte Jikto apropriada fará um escaneamento de vulnerabilidades em um web site diferente. Os logs daquele site levarão de volta ao usuário e não necessariamente ao servidor onde a fonte Jikto estava localizada. Assim, desde que o escaneamento de vulnerabilidade esteja realmente sendo realizado por um usuário final, a localização do atacante será eficazmente escondida.

A Symantec espera que novas pesquisas continuem a ser feitas sobre novas técnicas para despistamento de SOP. Ainda não está claro se as vulnerabilidades encontradas serão exploradas em seu estado natural em larga escala.

Diversificação no uso de bots

Bots são programas que instalados de maneira disfarçada na máquina do usuário a fim de permitir que outro usuário não autorizado possa controlar remotamente o computador. Eles permitem que um atacante possa controlar o sistema visado através de um canal de comunicação chamado IRC. Esses canais permitem que um atacante remoto controle um grande número de computadores comprometidos através de um único e confiável canal em uma rede bot, que pode então ser usado para lançar ataques coordenados.

Bots permitem uma vasta gama de funcionalidades e a maior parte delas pode ser atualizada para realizar novas tarefas através do download de novos códigos e características. Eles podem ser usados por atacantes externos para realizar ataques de negação de serviço contra o site de uma organização. Além do mais, bots dentro da rede de uma organização podem ser usados para atacar sites de outras organizações, o que pode trazer serias consequências comerciais e legais. Bots podem ser usados pelos atacantes para colher informação confidencial de computadores comprometidos, o que pode levar ao roubo de identidade. Eles também podem ser usados para distribuir spam e para realizar ataques de phishing, tanto quanto para spyware, adware, aplicações enganosas.

Bots tendem a ser “usuários precoces” de uma nova funcionalidade porque devido a seu design, eles podem incorporar facilmente novos códigos através de redes de bot amplamente dispersas. Como tal, eles podem ser usados como testes de ambientes, utilizando novas funcionalidades de códigos maliciosos em uma variedade de alvos antes de fazer uso amplo deles. Por causa dessa capacidade, a Symantec acredita que os bots e redes de bots tenderão a ser usados em um número de maneiras cada vez maior num futuro próximo.

Por exemplo, bots podem ser usados em ataques de phishing do lado cliente contra usuários ou proprietários legítimos de um computador infectado, código malicioso em um computador infectado poderia ser usado para imitar o web site legítimo de uma organização cuja marca está sendo usada em ataques de phishing. Como resultado a vítima escolhida, poderia ser persuadida a revelar informação de identidade pessoal, que poderia ser usada posteriormente em atividade fraudulenta. Esta abordagem permite que phishers burlem alguns mecanismos anti-phishing tradicionais. Além disso, um phisher usando esta técnica não teria que depender de um web site que poderia ser desativado caso fosse descoberto.

Em outro exemplo, bots podem dar aos atacantes acesso específico a computadores infectados que os atacantes podem então usar em seu proveito. Proprietários de bot podem extrair informação de identificação de localização tais como nomes de domínios de computadores infectados tais como nomes de domínios de computadores infectados e depois anunciar que eles controlam um computador dentro de uma organização

específica. Partes com interesse na organização visada podem pagar para o uso do computador comprometido para juntar informação ou para conduzir ataques. Esta abordagem poderia aumentar enormemente o risco de infecção por bots em uma organização.

Em um exemplo final de nova funcionalidade de códigos maliciosos, bots podem ser usados para aumentar artificialmente o tráfego aparente de certos web sites. Em uma variação do conceito tradicional de golpe do click, os bots podem ser usados para seqüestrar browsers, direcionando - os para sites que permitem que os usuários se inscrevam e votem em web sites recomendados. A idéia por trás disso é a de falsamente melhorar as pontuações de mecanismos de busca, dando a impressão de alto tráfego a um site em particular, desse modo conduzindo tráfego para aquele site. Isso poderia ser então usado para gerar rendimentos provenientes de propaganda ou para enviar códigos maliciosos, o que poderia ser usado para atividades fraudulentas posteriores.

Sobre a Symantec

A Symantec é um líder global em softwares de infra-estrutura, permitindo que usuários e empresas sintam-se confiantes em um mundo conectado. A Symantec ajuda seus clientes a proteger sua infra-estrutura, informação e interações através do provimento de softwares e serviços voltados a riscos de segurança, disponibilidade, compliance e desempenho. Sediada em Cupertino, Califórnia, a Symantec opera em 40 países. Mais informação encontra-se disponível em www.symantec.com.

Copyright © 2007 Symantec Corporation. Todos os direitos reservados . Symantec, o logo da Symantec, BugTraq, e o Symantec Brightmail AntiSpam são marcas registradas da Symantec Corporation ou de suas afiliadas nos EUA e em outros países. Apple e QuickTime são marcas registradas da Apple Inc., registradas nos EUA e em outros países. Safari é uma marca registrada da Apple Inc. Microsoft, ActiveX, Internet Explorer, e Windows Media são ou marcas registradas ou marcas registradas da Microsoft Corporation nos Estados Unidos e/ou outros países. Sun, Java, e Solaris são marcas registradas da Sun Microsystems, Inc. nos EUA e em outros países. Outros nomes podem ser marcas registradas de seus respectivos proprietários.