

IBM Global Technology Services

Janeiro de 2009

**IBM Internet Security Systems
Relatório de Tendências e Riscos da X-Force®
2008**

Índice

Visão Geral	4
Destaques de 2008	5
Vulnerabilidades	5
Ameaças de Segurança Relacionadas com a Web.....	6
Spam e Phishing	7
Malware	7
Economia da Exploração: O que não aconteceu em 2008 e por que	8
Análise Comercial de Ameaças à Segurança no Computador	8
Economia do Crime 101	10
Oportunidades Criminosas	10
Custos do Crime	10
Exemplos	11
Execução Remota do Código do Microsoft Snapshot Viewer ActiveX Control	11
HMAC Security Bypass do SNMPv3	13
Execução Remota de Código do Microsoft IIS HTML Encoded ASP.....	15
Execução Remota de Código do Microsoft Windows Server Service.....	16
DNS Cache Poisoning	17
Conclusão	20
Vulnerabilidades	22
Contagem de Descobertas de Vulnerabilidades em 2008	22
Tempo para a Descoberta de Vulnerabilidades	23
Descobertas de Vulnerabilidades por Severidade	24
Pontuação Básica do CVSS.....	25
Pontuações Temporais do CVSS.....	27
Fornecedores com a Maioria das Descobertas de Vulnerabilidades	28
Novos Fornecedores na Lista dos Principais	29
Correções Disponíveis de Vulnerabilidades	31
Vulnerabilidades Exploráveis Remotamente	32
Consequências da Exploração	33
Vulnerabilidades de Aplicativos da Web	35
Vulnerabilidades de Aplicativos da Web por Categorias de Ataque	36
Ataques de Exploração ativa e Injeção SQL Automática em 2008.	40
Não há Correção Disponível	41
Web sites Bons Usando Controles de ActiveX Ruins	42
Sistemas Operacionais Mais Vulneráveis	44
Vulnerabilidades e Exploits do lado do Cliente, do Navegador e Outros	45

Vulnerabilidades do lado do Cliente – Os Navegadores estão Melhorando	45
Descobertas de Vulnerabilidades de Nível Crítico e Alto em Aplicativos Predominantes	46
Vulnerabilidades de Navegador e Plug-in – Queda nas Descobertas do ActiveX	48
Disponibilidade do Código de Exploração no Dia Zero	50
Alvos de Exploit: do Sistema Operacional ao Navegador e Além	51
Tendências da Exploração do Navegador da Web	51
Exploits Mais Populares	52
Kits de Ferramenta de Exploit Mais Populares (2º semestre de 2008)	53
Ofuscamento	54
Exploração e Ofuscamento de PDF	54
Atividade Global de Ataques do Lado do Cliente	55
Exploits de Web Sites Maliciosos	55
Países que Hospedam a Maior Parte dos Web Sites Maliciosos	57
Spam	58
Volume de Spam	59
Mais tendências rumo a um spam mais simples	60
Spam com URL	60
Ascensão e Queda de Spam de Texto Simples	61
Domínios Comuns em Spam de URL	62
Top Level Domains Comuns em Spam de URL	64
Por que .com? / Por que .cn?	67
Expectativa de Vida de URLs com Spam	68
Spam – País de Origem	69
Spam – Tendências do País de Origem	70
URLs com Spam – País de Origem	71
URLs com Spam – Tendências do País de Origem	72
Spam – Tamanho Médio de Bytes	74
Spam – Linhas de Assunto Mais Populares	74
A Remoção da McColo e Seu Impacto sobre o Spam	76
Mudanças na Distribuição Internacional de Spam	76
Mudanças no Conteúdo de Spam	78

Relatório de Tendências e Riscos da X-Force® 2008

Página 1

Visão Geral

A equipe de pesquisa e desenvolvimento de Internet Security Systems X-Force® da IBM descobre, analisa, monitora e registra uma vasta gama de ameaças e vulnerabilidades de segurança. De acordo com as observações da X-Force, muitas tendências novas e surpreendentes vieram à tona durante o ano de 2008. Esperamos que as informações apresentadas neste relatório, sobre estas tendências, proporcionem uma base sólida para o planejamento dos seus esforços de segurança da informação neste e nos próximos anos.

A indústria da segurança dedica muito esforço à avaliação técnica das ameaças à segurança, examinando, por vezes durante longo tempo, o perigo potencial de cada item para as empresas e os consumidores. No entanto, os atacantes criminosos em busca de lucros consideram coisas que nem sempre são levadas em conta pela indústria da segurança, como o custo da monetização e a lucratividade em geral.

Muitas questões de segurança foram alardeadas em 2008, algumas das quais nunca passaram de exploração da massa. A primeira seção deste relatório, “Economia da Exploração: o que não aconteceu em 2008 e por que”, na página 5, discute esta questão em detalhes e apresenta algumas lições que podem ajudar a indústria a avaliar melhor estes tipos de problemas de segurança no futuro.

Os criminosos da computação procuram informações que possam transformar em lucros rapidamente. De modo geral, esta ativação acelerada do investimento significa informações sobre cartões de créditos e credenciais de acesso às contas bancárias dos consumidores. Embora muitas vezes os atacantes encontrem formas de colher enormes quantidades deste tipo de dados dos servidores e redes corporativas, grande parte destas informações são roubadas por spyware, executado diretamente nos PCs dos usuários finais.

As empresas que usam mecanismos avançados de correção e proteção podem criar, também, mais obstáculos (custos elevados de monetização e lucratividade mais baixa) para os atacantes. Os consumidores, por outro lado, com sua falta de proteção, comportamentos corriqueiros de correção e falta geral de perícia em segurança, continuam a ser alvos fáceis. A exploração em massa continuada de problemas de navegador, principalmente controles de ActiveX, são indicadores claros deste problema. Os novos vetores de exploração, como o uso de arquivos PDF e aplicativos de multimídia como o Flash, que incluem exploits embutidos, tornaram-se mais proeminentes do que nunca, com tendência a subir até o final do ano.

Relatório de Tendências e Riscos da X-Force® 2008

Página 2

Determinados tipos de aplicativos corporativos, mais precisamente software construído pelo cliente como aplicativos da Web, continuam a representar um alvo altamente lucrativo e econômico para os atacantes criminosos. O número crescente de novas vulnerabilidades, a maioria delas ainda sem correção, ligadas a centenas de milhares de aplicativos customizados da web que também são vulneráveis (vulnerabilidade esta dificilmente revelada, menos ainda sua correção), tornou-se o calcanhar de Aquiles da segurança nas empresas. Os atacantes continuam a mirar as vulnerabilidades dos aplicativos da web, principalmente a injeção SQL, para semear malware em usuários sem malícia que visitam Web sites vulneráveis.

Destaques de 2008

Vulnerabilidades

- *2008 provou ser o ano mais ativo na história da X-Force em termos de vulnerabilidades crônicas – representando um aumento de 13,5% em comparação a 2007.*
- *A severidade geral das vulnerabilidades aumentou, apresentando severidades de nível alto e crítico de até 15,3% e de nível médio de até 67,5%.*
- *De forma idêntica a 2007, perto de 92% das vulnerabilidades de 2008 podem ser exploradas à distância.*
- *De todas as vulnerabilidades reveladas em 2008, apenas 47% puderam ser resolvidas por intermédio de correções dos fornecedores. Os fornecedores nem sempre voltam atrás para corrigir as vulnerabilidades do ano anterior. Quarenta e seis por cento das vulnerabilidades de 2006 e 44% das vulnerabilidades de 2007 foram abandonadas, sem que houvesse correção disponível no final de 2008.*
- *As duas maiores categorias de vulnerabilidades em 2008 estavam relacionadas a aplicativos da web em 55% dos casos e as vulnerabilidades que afetam software de PC giravam em torno de 20%.*
- *Os sistemas operacionais da Apple e o kernel básico do Linux dominaram as principais marcas de descobertas de vulnerabilidades em sistemas operacionais nos últimos três anos.*

Ameaças de Segurança Relacionadas com a Web

o O número de sites maliciosos novos na Web só no quarto trimestre de 2008 ultrapassou o total observado no ano inteiro de 2007 em 50%. Ano passado, A China substituiu os EUA no posto de hóspede mais prolífico de sites maliciosos na Web.

o Até mesmo os sites saudáveis da Web estão enfrentando mais problemas. Os aplicativos da Web, em particular, estão cada vez mais vulneráveis, além de serem alvos altamente lucrativos para ajudar o submundo do crime a construir exércitos de botnets.

o Os spammers estão se voltando para a Web. O spam de URL (um e-mail com spam que tem pouco mais do que um link com uma página da Web que distribui a mensagem com spam) assumiu a liderança este ano; e os Spammers estão usando cada vez mais nomes de domínios familiares, como sites de notícias e blogs da Web, para hospedar seus conteúdos.

o Os aplicativos da Web, em geral, se transformaram no calcanhar de Aquiles da Segurança Corporativa de TI. Aproximadamente 55% de todas as descobertas de vulnerabilidade em 2008 afetam aplicativos da Web, e este número não inclui os aplicativos da Web desenvolvidos sob encomenda (apenas pacotes fabricados em série). Setenta e quatro por cento de todas as vulnerabilidades nos aplicativos da Web revelados em 2008 ainda não tinham correção no final de 2008.

o Ano passado, a injeção SQL deu um salto de 134% e substituiu o scripting de sites cruzados como o tipo predominante de vulnerabilidade de aplicativos da Web.

o A exploração de Web sites vulneráveis à injeção SQL aumentou de alguns milhares por dia, em média, quando começaram a acontecer no início de 2008, para centenas de milhares por dia, no final de 2008.

o Alem destas vulnerabilidades, muitos Web sites solicitam o uso de controles ActiveX vulneráveis conhecidos, deixando os visitantes do site que não têm navegadores atualizados numa posição difícil.

o Embora o número de vulnerabilidades que afetam os navegadores da Web tenha caído em comparação a 2007, elas continuam a ser o principal alvo de exploração. Novas categorias de ameaças que afetam os clientes estão em ascensão, especificamente nas áreas de documentos maliciosos, aplicativos multimídia e provavelmente aplicativos Java, que são fáceis de hospedar na Web.

Relatório de Tendências e Riscos da X-Force® 2008

Página 4

Spam e Phishing

o O fechamento da McColo teve o maior impacto sobre a atividade do spam em 2008, não apenas afetando a quantidade, como também o tipo de spam enviado e os países que o enviam com maior frequência.

o Embora o volume de spam tenha caído após o fechamento, a X-Force espera que volte ao normal no primeiro trimestre de 2009.

o O spam simples (baseado em texto ou na URL) substituiu o spam complexo (PDF, imagem, etc.) em 2008, com ênfase no spam de URL perto do final do ano. Os spammers usam cada vez mais domínios familiares de URL, como sites de blogs e de notícias, para hospedar mensagens com spam.

o Embora a maior parte das URLs com spam use o TLD (Top Level Domain) .com, o aumento consistente no uso de .cn é evidente, e, quando se trata de URLs maliciosos, o número hospedado na China ultrapassou o dos EUA este ano.

o Mais de 97% das URLs com Spam permanecem ativas durante no máximo uma semana.

o Em termos de servidores que enviam spam, a Rússia ultrapassou os EUA em 2008, e foi responsável por 12% de todo o spam enviado no ano passado.

o As linhas de assunto mais populares de phishing e spam já não são tão populares. As dez linhas mais usadas de 2008 cresceram numa percentagem menor em comparação a 2007. Os spammers e phishers também estão se tornando mais granulares e alcançáveis, tendo mais trabalho, na essência, para atingir mais alvos. Em 2007, as linhas de assunto mais populares de phishing representavam cerca de 40% de todos os e-mails com phishing. Em 2008, as linhas de assunto mais populares reuniram apenas 6,23% de todas as linhas de assunto de phishing.

o Outra tendência que se desenvolveu em 2008 é o foco na ação do usuário. Em vez de ter um assunto genérico, tipo "alerta de segurança", os phishers tentam comprometer o usuário com alguma ação, tipo reativar uma conta que foi suspensa ou atualizar os dados de sua conta.

o A maior parte do phishing – aproximadamente 90% – objetivava instituições financeiras. Mais de 99% dos alvos de phishing financeiro estão na América do Norte ou na Europa, a maioria situada na América do Norte (58,4%).

Malware

o Quarenta e seis por cento de todo o malware colhido em 2008 eram cavalos de tróia. Os cavalos de tróia que objetivam usuários de jogos on-line (Onlinegames, Magania) e operações bancárias on-line (Banker e Banload) continuam predominantes durante o ano inteiro, o que indica que estes grupos específicos de usuários foram altamente visados em 2008.

Economia da Exploração: O que não aconteceu em 2008 e por que

“Amadores Estudam Criptografia; Profissionais Estudam Economia” é o título provocativo de um dos capítulos de uma publicação recente intitulada “Nova Escola de Segurança da Informação”, de autoria de Adam Shostack e Andrew Stewart. O título deste capítulo realça um ponto cego que atualmente contamina alguns cantos da indústria da segurança. É claro que há muitos profissionais sérios apresentando contribuições importantes através de um melhor entendimento da natureza técnica de problemas de segurança do computador, porém o foco não está suficientemente centrado na forma como os incentivos econômicos e as exterioridades interagem com aqueles problemas técnicos.

Quando deixamos de levar em conta o contexto econômico no qual as vulnerabilidades da segurança do computador existem, terminamos priorizando as ameaças erradas. Como a X-Force examinou as vulnerabilidades mais divulgadas em 2008, observamos que um número de ameaças críticas não se materializou em ataques amplamente espalhados no campo. Um exame mais detido naquelas ameaças revela algumas lições que podem ajudar a nossa indústria a avaliar melhor os futuros problemas de segurança.

Análise Comercial de Ameaças à Segurança no Computador

No presente, a indústria da segurança prioriza as ameaças quase que inteiramente com base nas medidas técnicas dos riscos que elas apresentam. O Common Vulnerability Scoring System (CVSS) é o sistema padrão de priorização de ameaças deste segmento. As métricas que ele considera para sua pontuação básica se concentra nos aspectos técnicos da vulnerabilidade. Elas levam em conta:

- *O nível de dificuldade para acessar a interface de software vulnerável*
- *O impacto que um ataque bem sucedido tem sobre a confidencialidade, a integridade e a disponibilidade dos sistemas vulneráveis*
- *A disponibilidade e a confiabilidade públicas do código de exploração*
- *A disponibilidade de correções ou soluções alternativas*

Embora algumas considerações econômicas estejam inseridas nos fatores ambientais de CVSS, os fatores de cada empreendimento são entendidos como únicos e não são incorporados nas pontuações básicas do CVSS que aparecem nos bancos de dados de vulnerabilidade de segurança da indústria. E mais: o foco das considerações econômicas está inteiramente dirigido para os custos que um ataque bem sucedido podem impor a uma organização.

Embora todos os fatores considerados pelo CVSS sejam importantes, o que os pontos do sistema deixam de capturar é a oportunidade econômica que uma vulnerabilidade apresenta para um atacante. Os dias de amadores, estudantes universitários ou hackers em viagens divertidas pelos sistemas de informações corporativas já estão bem longe. A motivação dos atacantes de hoje é econômica. São organizações criminosas internacionais que fazem do roubo de informações financeiras e identidades um meio de vida. A ameaça hoje é bem mais sofisticada e muito mais perigosa do que as ameaças na segurança de outrora, mas em alguns casos, são mais previsíveis. Enquanto o hacker amador pode estar interessado numa vulnerabilidade na segurança que chega, os criminosos alarmantes da informática estão interessados principalmente em vulnerabilidades que proporcionem um significativo retorno sobre o investimento.

**Pontos do CVSS deixam de capturar a oportunidade econômica
que as vulnerabilidades apresentam aos atacantes.**

O resultado desta nova realidade é que houve diversas vulnerabilidades este ano que receberam pontuações muito altas no CVSS e espalharam alarme por uma vasta área da indústria da segurança. No entanto, elas não foram amplamente exploradas durante sua disseminação. Na maior parte dos casos, essas vulnerabilidades não se enquadraram bem nos modelos comerciais correntes dos criminosos da informática. Os departamentos de TI não devem ignorar vulnerabilidades que apresentem sérios riscos à sua infraestrutura simplesmente porque eles acham que aquelas vulnerabilidades não se tornaram largamente populares junto ao crime organizado. Adversários altamente sofisticados podem usar vulnerabilidades raramente exploradas nos ataques planejados. No entanto, uma consideração mais cuidadosa sobre a forma como as vulnerabilidades se enquadram nos modelos comerciais de organizações criminosas ajudará a priorizar melhor os esforços de proteção e correção de TI.

Economia do Crime 101

Num nível microeconômico básico, o entendimento da oportunidade de um criminoso da informática advém de considerar-se o montante de receita que pode ser gerada com a exploração de uma vulnerabilidade em relação ao custo de sua execução. Obviamente, as vulnerabilidades que apresentam oportunidade de receita elevada a um custo baixo tendem a ser populares entre os atacantes. Tanto a receita (oportunidade) quanto o custo são formados por um conjunto complicado de componentes, e alguns deles podem ser influenciados pela indústria da segurança.

Oportunidades Criminosas

As receitas reais que podem ser geradas com a exploração de uma vulnerabilidade resultam da combinação do tamanho da base instalada dos hosts vulneráveis e o valor que o atacante dá ao poder de controlar cada host, normalmente em função das informações que os hosts contêm e do preço que o atacante pode pedir pelas informações no mercado negro. Logo que uma vulnerabilidade é revelada, a base instalada de hosts vulneráveis pode ser enorme, e se o valor de controlar aqueles hosts também é grande, o atacante tem uma oportunidade teórica significativa de receita. Este tipo de situação pode motivar esforços por parte da indústria da segurança para espalhar correções rapidamente e reduzir o tamanho da base instalada. Se a indústria for eficaz, a oportunidade total real de receita pode tornar-se muito diminuta para que os ataques se materializem. Por outro lado, podem haver casos em que a base instalada de hosts vulneráveis seja grande, porém o valor de controlar o tipo de host que normalmente executa o software vulnerável é pequeno, e assim sendo os atacantes têm pouco incentivo para explorar a vulnerabilidade, independentemente do que a indústria da segurança fizer para corrigi-la.

Custos do Crime

O custo de gerar receitas com a exploração de vulnerabilidades também é composto por uma série de fatores. Dois aspectos do custo que o CVSS captura bem são o custo de obtenção de um exploit, que depende dele estar ou não disponível publicamente, e da dificuldade associada com o seu uso. O CVSS também captura o impacto do exploit – o que o atacante obtém – em termos técnicos. Todavia, um atacante motivado financeiramente tem que reverter o que quer que tenha sido causado pelo acesso ou a degradação no desempenho pelo ataque em dinheiro. A monetização de alguns tipos de acesso é mais cara do que a de outros.

Assim como os negócios lícitos, as organizações criminosas têm processos operacionais que são construídos em torno de conjuntos reiteráveis de circunstâncias e tarefas automatizáveis. Para os criminosos, as vulnerabilidades que se encaixam nos processos existentes e que podem alavancar a automação existente são fáceis de monetizar. As vulnerabilidades que exigem o desenvolvimento de novos processos ou software têm uma probabilidade bem menor de apresentar uma oportunidade atraente para criminosos, principalmente se elas representarem um conjunto atípico de circunstâncias que não têm grande probabilidade de serem repetidas no futuro. Mesmo quando não faz sentido para os criminosos desenvolver uma nova metodologia de ataque para explorar uma nova classe de vulnerabilidades, os ataques de grande espectro normalmente demorarão mais para emergir do que as vulnerabilidades que se encaixam diretamente no processo em uso.

Exemplos

Para entender melhor de como esses fatores afetam a exploração, podemos considerar algumas das grandes descobertas de vulnerabilidades de 2008. O que primeiro faz sentido é considerar uma vulnerabilidade que foi largamente explorada.

Execução Remota do Código do Microsoft Snapshot Viewer ActiveX Control
À vulnerabilidade do Microsoft Snapshot Viewer ActiveX Control (CVE-2008-2463) foi atribuída uma pontuação básica do CVSS de 7,5 pelo NIST (Instituto Nacional de Padrões e Tecnologia). Ela foi relatada pela primeira vez ao público pela Microsoft no dia 7 de julho de 2008, quando a empresa soube do alvo de exploração a ser disseminada. Infelizmente, esta vulnerabilidade é fácil de explorar com segurança, já que não se trata de um excesso de buffer que exige o uso de offsets específicos da versão, e sim de uma interface que permite o download de um arquivo arbitrário da Internet e sua colocação em qualquer lugar no computador da vítima, inclusive na pasta de inicialização ou no lugar de um arquivo de sistema.



Figura 1: Probabilidade de Exploração de Vulnerabilidade do Snapshot Viewer.

No dia 10 de julho, um exploit da vulnerabilidade já tinha sido incorporado no kit de ferramentas de exploit da Web, inclusive o NeoSploit. Esses kits de ferramentas são usados por organizações criminosas para automatizar a tarefa de infectar um computador. Quando os PCs vitimados se encontram com a página errada da Web são redirecionados para um servidor em que esteja hospedando um kit de ferramentas, o qual colherá informações do navegador e de outras versões, do host da vítima, e transmitirá um exploit para o navegador desta, o qual agirá contra o software que a vítima está executando.

Um problema com controles do ActiveX é que às vezes eles não têm que ser instalados no computador alvo para que um atacante tire partido deles. É comum que um servidor da Web instrua um navegador para baixar novos controles de ActiveX quando o controle necessário ainda não está instalado. Portanto, tudo o que o atacante tem que fazer é atrair o navegador do usuário para instalar um controle vulnerável, e depois direcionar o navegador para um exploit daquele controle, quando ele já tiver sido instalado. Neste caso, o controle Snapshot Viewer era marcado com um certificado digital da Microsoft. Para um usuário final, ver o prompt de instalação de algo novo fica menos suspeito quando ele aparece como proveniente de uma entidade em que confia.

Tuesday, July 8 Exploit Code Published	Terça-feira, 8 de julho Código de Exploit Publicado
Monday, July 7 Vulnerability Disclosure & Targeted Exploitation	Segunda-feira, 7 de julho Descoberta de Vulnerabilidade e Alvo da Exploração
Thursday, July 10 Mass Exploitation through Toolkits Begins	Terça-feira, 10 de julho Começa a Exploração em Massa por meio de Kits de Ferramentas

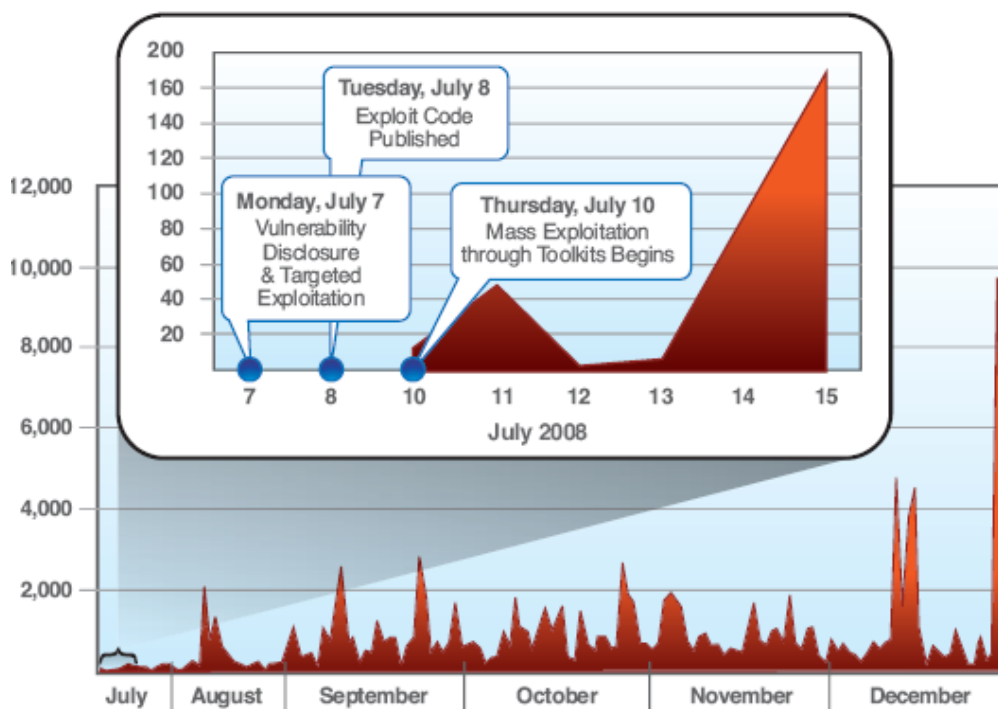


Figure 2: Exploração de Controle do Microsoft Snapshot Viewer ActiveX

No dia 24 de julho, a IBM estava acompanhando mais de 50 hosts que exploravam ativamente o problema. Em 1º de agosto, novas variáveis foram relatadas, as quais forçavam os usuários que não tinham o controle ActiveX vulnerável a instalá-lo e assim acessavam o exploit em massa, expandindo a base instalada de máquinas potencialmente vulneráveis. A Microsoft publicou correções para a vulnerabilidade no dia 12 de agosto.

A vulnerabilidade do Snapshot Viewer era popular entre os atacantes, não apenas porque era fácil de explorar, mas porque se adaptava perfeitamente aos processos estabelecidos e às ferramentas de software que empregavam. As vulnerabilidades são quase sempre relatadas nos controles de ActiveX e os atacantes estão acostumados a incorporar exploits nos kits de ferramentas de exploit da Web e a usá-los para propagar spyware que coleta credenciais financeiras. Portanto, neste caso, o custo de exploração era baixo, assim como o custo da monetização. A base instalada era essencialmente infinita, já que os atacantes podiam deslocar o controle marcado pela Microsoft para qualquer pessoa que permitisse sua instalação. O resultado é que uma grande oportunidade de receita combinada com um baixo custo de monetização leva a uma grande quantidade de exploração que ainda não mostra sinais de queda, conforme nos mostra a Figura 2. Para maiores informações sobre a exploração do ActiveX e as vulnerabilidades do cliente no horizonte, veja "Vulnerabilidades e Exploits do Navegador e Outras Vulnerabilidades e Exploits do Cliente", na página 41

HMAC Security Bypass do SNMPv3

Compare a vulnerabilidade do Snapshot Viewer com a do SNMPv3 HMAC Authentication Vulnerability (CVE-2008-0960). Originalmente, o NIST atribuiu a esta vulnerabilidade uma pontuação básica do CVSS de 6,8, fazendo com que muitos analistas de segurança a ignorassem. Depois, a pontuação foi revisada e modificada para 10, quando todas as implicações ficaram claras. Esta vulnerabilidade é muito fácil de explorar, exigindo apenas 256 pacotes para acessar qualquer interface do SNMPv3 protegida por senha. Além disto, pode-se fazer o download do modelo de código de exploit da Internet. As Consequências de segurança podem ser significativas dependendo do que o SNMPv3 foi configurado para executar. Os roteadores da Internet, que os atacantes conseguem reconfigurar usando esta interface para desorganizar, espionar ou modificar o tráfego na Internet, são particularmente preocupantes. Considerando-se o potencial desta vulnerabilidade, a facilidade para explorá-la, e o enorme tamanho da base instalada para o SNMP, era de se esperar que a exploração fosse difundida, ou que houvesse, pelo menos, sondagens e tentativas de exploração, embora a materialização fosse mínima.

Isto se deve ao fato de que mesmo que esta vulnerabilidade seja fácil de explorar, é difícil monetizar um ataque bem sucedido. Este tipo de vulnerabilidade é um caso especial que não se adequa facilmente aos modelos comerciais dos grupos de criminosos organizados, que estão tentando lucrar com os problemas de segurança dos computadores. Um ataque real idealizado para coletar informações financeiras usando esta vulnerabilidade teria dois estágios. O primeiro estágio envolve reconfigurar um roteador para encaminhar o tráfego através de uma rede controlada por um atacante. No entanto, como a maior parte das transações financeiras pela Internet são criptografadas, é necessário um segundo estágio, no qual o atacante manipula determinado tráfego da rede, como o DNS, para direcionar a vítima a sites de phishing controlados pelos atacantes, ou para persuadir a vítima a baixar um malware. Em última análise, este tipo de ataque é muito complicado, porque envolve o desenvolvimento de um conjunto de técnicas e software especificamente projetados para alavancar esta espécie de vulnerabilidade. Como hoje há correções disponíveis, a janela de oportunidades para explorar esta vulnerabilidade está se fechando, portanto temos um custo muito alto de monetização associado, com uma oportunidade de receita acanhada. O resultado é pouca ou nenhuma exploração.



Figure 3: Probabilidade de Exploração do HMAC Security Bypass

Execução Remota de Código do Microsoft IIS HTML Encoded ASP

Alguns casos devem ter desaparecido de qualquer forma. Em fevereiro, a Microsoft corrigiu uma vulnerabilidade na execução remota de código em ASP (CVE-2008-0075), que também obteve 10 pontos no CVSS. Este ataque proporciona total controle sobre um servidor da Web vulnerável, algo em que os criminosos da informática estão muito interessados, uma vez que lhes possibilita redirecionar usuários para seus kits de ferramentas de exploit. Um exploit no CORE IMPACT demonstra que a vulnerabilidade é explorável, e uma análise pública do bug pela H.D. Moore apresenta alguns detalhes técnicos. Contudo, nunca emergiu um exploit público, e até a data desta publicação a X-Force não tem ciência de quaisquer exploits privados que estejam sendo usados em ataques. Talvez a razão de nenhum exploit público ter sido desenvolvido até hoje para esta vulnerabilidade é o fato da injeção SQL ser bem mais eficaz enquanto técnica para o desenvolvimento de exploit para que o esforço valha à pena. Muitos Web sites desenvolvidos em todos os tipos de linguagens são vulneráveis a injeções SQL, e eles foram extremamente usados este ano para injetar redirecionadores de JavaScript nas páginas da Web que entregam vítimas sem malícia nos braços de espera dos kits de ferramentas de exploit de navegador. A ascensão na exploração está descrita em "Ataques com Exploração Ativa e Injeção SQL em 2008", na página 36.

Para contrastar, esta vulnerabilidade oferece uma oportunidade mais limitada, funcionando apenas contra páginas ASP que sejam projetadas para aceitar entrada formatada em Unicode e existe, também, aqui, alguma filtragem de caracteres em jogo, que pode frustrar a execução do código. Finalmente, uma oportunidade de receita baixa e um custo alto de desenvolvimento de exploit torna este ataque nada atraente diante das vulnerabilidades com injeção SQL espalhadas que são muito fáceis de explorar.

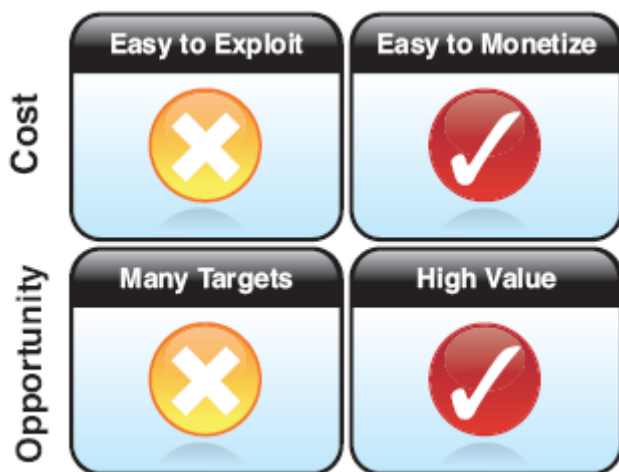


Figure 4: Probabilidade de Exploração do Microsoft IIS HTML Encoded ASP

Execução Remota de Código do Microsoft Windows Server Service

A vulnerabilidade do Servidor da Microsoft (CVE-2008-4250) também merece ser analisada. Esta vulnerabilidade também recebeu 10 pontos do CVSS e exatamente como uma worm (Gimmiv) estava sendo explorada de forma limitada antes que fosse revelada ao público. Obviamente, a oportunidade financeira aqui para os caras maus era gigantesca, e a revelação pública de diversas iterações de código de exploração com prova-de-conceito facilitou a exploração. De fato, havia até mesmo relatos de ferramentas de geração de exploração automatizada para esta vulnerabilidade.

Nos anos passados, vulnerabilidades similares de Microsoft RPC conduziram a eclosões de worms que se propagaram muito rapidamente. Por exemplo, no verão de 2003, a worm Blaster começou a explorar uma vulnerabilidade do RPC DCOM cerca de um mês depois que foi corrigida. De acordo com a pesquisa da época, o Blaster alcançou seu pico de propagação dentro de 8 horas de seu lançamento. A worm Conficker, explorando a vulnerabilidade do Server Service, seguiu um padrão diferente. Primeiro foi relatada no final de novembro, também cerca de um mês após o lançamento inicial da correção, mas se espalhou muito lentamente. A worm não atingiu completamente seu ritmo até janeiro, e por esta época novas variáveis estavam sendo liberadas, que empregavam diversos métodos de propagação, como a quebra da senha compartilhada de SMB.

A culpa pelo sucesso do worm Conficker foi largamente depositada aos pés de uma pequena porção de empresas (foram reportadas cerca de 3 em 10) que desligaram o Windows Update automático e operam ciclos de teste de compatibilidade muito longos antes de produzir as correções de segurança. De acordo com os relatórios, a maioria dos clientes receberam rapidamente a correção, e as empresas certamente tiveram tempo de implementar as correções, assinaturas de IPS, ou ambos. Estes fatores contribuíram para a lenta propagação da worm em relação às experiências anteriores. De fato, se não fosse pela adição de métodos secundários de propagação (compartilhamento de rede, quebra de senha e mídia removível, todos facilmente acessáveis em ambientes corporativos), esta worm talvez não teria se espalhado tanto, afinal.

Embora críticas, ainda são descobertas vulnerabilidades transformáveis em worms; grandes erupções como a da Conficker são bem menos comuns hoje do que eram há alguns anos. Quando acontecem, surgem de forma mais lenta, o que atesta os esforços feitos há alguns poucos anos na indústria de TI para melhorar a resposta à vulnerabilidade e a segurança geral do computador. No entanto, o sucesso fundamental do Conficker é a evidência de que ainda há muito por fazer.

DNS Cache Poisoning

Isto nos lembra a maior história de segurança do computador, ocorrida em 2008: a vulnerabilidade do DNS Cache Poisoning, descoberta por Dan Kaminsky (CVE-2008-1447). O NIST deu a esta uma pontuação básica de 7,5 do CVSS, mas a ampla atenção recebida da mídia por esta vulnerabilidade deixou claro que a indústria da informática a considerou uma ameaça muito séria. Um esforço maciço foi empregado para atualizar a infraestrutura de DNS da Internet, mas, de acordo com um estudo realizado pela The Measurement Factory, um terço de todos os servidores de DNS ainda eram vulneráveis em outubro. Diferentes servidores de DNS servem populações de usuários de diversos tamanhos, mas era de se esperar que um terço de todos os servidores de DNS, representando um grupo suficientemente grande de prováveis vítimas, formasse um alvo atraente, e como há exploits públicos disponíveis, não seria tão difícil vencer o ataque. Mas estamos assistindo à disseminação de bem poucos ataques. Existe apenas um par de pequenas histórias de que temos notícia.

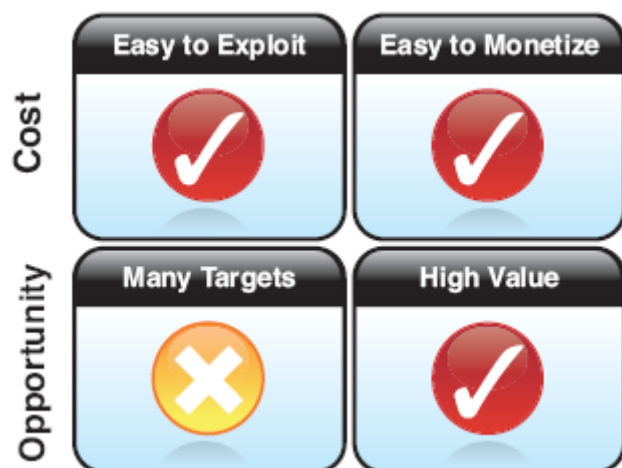


Figura 5: Probabilidade de Exploração do Microsoft Windows Server Service

Por que? A primeira pergunta a fazer é se este ataque se enquadra bem no atual empreendimento do crime. À primeira vista a resposta é sim. Nos últimos poucos anos, um cavalo de tróia conhecido como DNSChanger ou Zlob infectou suas vítimas usando um máscara de video codec. Entre outras coisas, este cavalo de tróia atualiza as configurações do servidor de DNS da vítima com endereços de IP controlados pelo atacante, redirecionando um determinado tráfego, inclusive resultados de busca, para alternar os destinos à escolha do atacante. O atacante monetiza este controle vendendo os olhos-de-cobra (*eyeballs*) desviados para anunciantes. Iterações mais recentes deste cavalo de tróia, lançadas este ano, se tornaram muito sofisticadas, atualizando as configurações de DNS em roteadores SOHO inseguros, e oferecendo serviços de DHCP, junto com as configurações do servidor malévolo de DNS, na LAN infectada. O ataque DNS Cache Poisoning é como um elogio natural a este modelo de negócio. Esta operação, especificamente, já tem fila de clientes para pagar por ela, e serve como um exemplo de que outros devem segui-la.

Mas há algumas diferenças importantes. Executar uma operação de varredura em grande escala na Internet em busca de servidores de DNS vulneráveis e atualizar sistematicamente seus conteúdos de cache para dirigir grandes quantidades de tráfego para anunciantes pagantes é um processo operacional significativamente diferentes daquele atualmente empregado por este grupo. Hoje, eles estão concentrados na manutenção do código de software do seu cavalo de tróia e operando alguns servidores de DNS perigosos. Da nossa perspectiva, leva tempo para que operações criminosas decidam adotar um processo operacional inteiramente novo como este, e para desenvolver confiança em seu uso. Eles têm que pensar bem nesta abordagem e consumir tempo desenvolvendo ferramentas. Por exemplo, as vulnerabilidades com injeção SQL foram entendidas durante quase 10 anos, mas como detalhamos mais à frente neste relatório, só nos últimos 12 meses teve início a exploração automática em grande escala dessas vulnerabilidades. O estado da injeção SQL não se deve a falta de oportunidade. Simplesmente leva tempo para amadurecer os métodos de exploração.

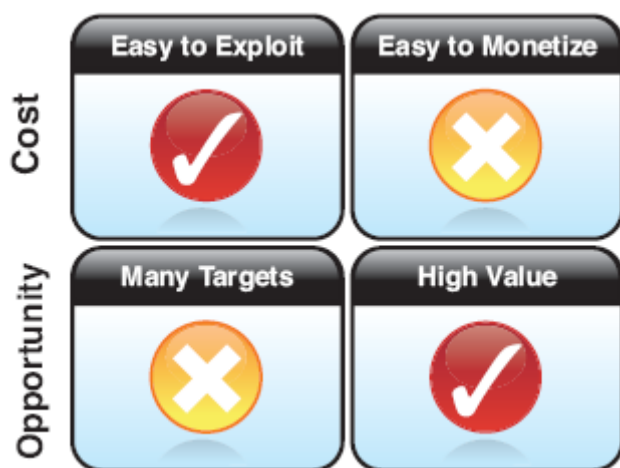


Figura 6: Probabilidade de Exploração do DNS Cache Poisoning

Além disto, pode haver uma diferença em termos de risco. O cavalo de tróia DNSChanger/Zlob não explora no presente vulnerabilidades de software, a menos que se responsabilize as senhas defeituosas nos roteadores SOHO. Suas primeiras vítimas instalaram o cavalo de tróia voluntariamente, em geral porque acreditavam que ele decodificaria vídeos pornográficos. Por inúmeras razões, suas vítimas devem ter se atrapalhado com a infecção e não queriam ir muito longe na sua resposta. Quando pressionados, os operadores do cavalo de tróia também podem argumentar que não cometeram nenhum crime, já que a instalação foi voluntária, embora a quebra das senhas do roteador SOHO guarde alguma dúvida sobre a credibilidade desta reivindicação. Apesar disso, um esforço em grande escala para explorar vulnerabilidades numa parte crítica da infraestrutura da Internet tem que bem mais audacioso. Os operadores de rede com vastos recursos investigatórios talvez queiram se aprofundar na resposta a uma ameaça como esta, e a resposta provável muda consideravelmente a equação econômica.

No entanto, é claramente possível fazer dinheiro envenenando caches de DNS e os criminosos sabem como fazê-lo. No início, esta vulnerabilidade representava um tremendo risco de longo prazo para a Internet. O esforço maciço empreendido neste verão para expandir o conhecimento e instalar correções reduziu bastante o universo de servidores vulneráveis. Por que este esforço para desenvolver uma técnica de ataque totalmente nova quando a que está em uso atualmente funciona tão bem e a nova oportunidade está encolhendo depressa? Se a população remanescente de servidores vulneráveis ficar por perto durante muito tempo, talvez possamos ver alguns atacantes colocarem seus pés na água. As coisas seriam muito diferentes se essas correções estivessem sendo adotadas mais lentamente e houvesse um *pool* maior de alvos sob a mira neste momento. Portanto, tanto alarde por parte da mídia durante o verão salvou a Internet? Talvez.

Conclusão

Para colocar todas essas questões em perspectiva, vamos considerá-las em conjunto. A Figura 7 representa cada problema em um dos quadrantes, com base na oportunidade que apresenta para o criminoso e o custo para realizá-la. Apenas os problemas colocados na parte superior direita tiveram sua exploração difundida. As outras não apresentaram uma oportunidade financeira suficiente ou seria muito dispendioso monetizá-las.

Se a indústria da segurança puder aprender a reconhecer vulnerabilidades que se encaixam no quadrante superior direito deste gráfico, será capaz de desenvolver um trabalho melhor, determinando quando uma correção de emergência é mais necessária diante de ameaças imediatas, quando o espalhamento da exploração de uma vulnerabilidade levará mais tempo para vir à tona e quando é pouco provável que sequer venha a emergir. Esta análise é de alguma forma ortogonal para a análise técnica em prática hoje, e acreditamos que o uso de tempo e recursos seria mais eficiente.

Monetization & Exploit Cost Opportunity	Oportunidade de Custo de Monetização e Exploração
LITTLE	POUCA
LOTS	MUITA
EXPENSIVE	DISPENDIOSA
CHEAP	ECONÔMICA

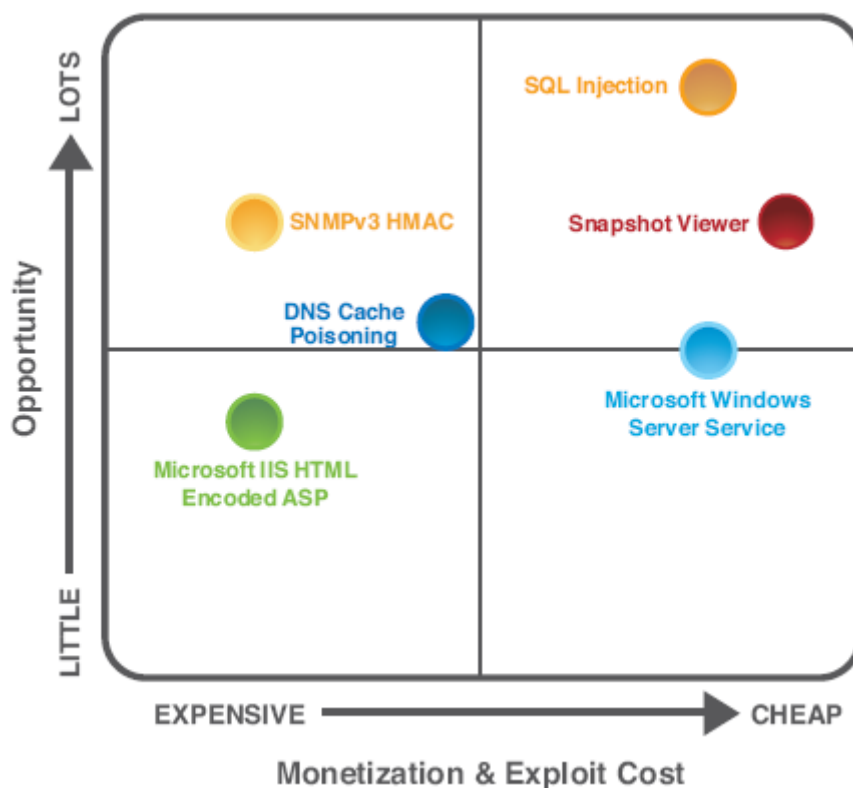


Figura 7: Quadrante de Probabilidade de Exploração

Mas, chega de falar do que não aconteceu em 2008. O restante deste relatório se dedica ao que aconteceu no ano passado e o que pode acontecer em 2009. À medida que percorrermos os tópicos, será útil manter em mente esta análise econômica. Não considere apenas a severidade e a facilidade de exploração de um problema de segurança, mas o fato é que os desafios de monetização e a oportunidade econômica determinarão se os criminosos irão ou não tirar partido da disseminação daquele problema.

Vulnerabilidades

Contagem de Descobertas de Vulnerabilidades em 2008

A X-Force analisou e documentou um número recorde de vulnerabilidades em 2008. As 7.406 novas vulnerabilidades representam 19% de todas as vulnerabilidades catalogadas desde que o Banco de Dados X-Force começou a ser formado, há mais de dez anos.

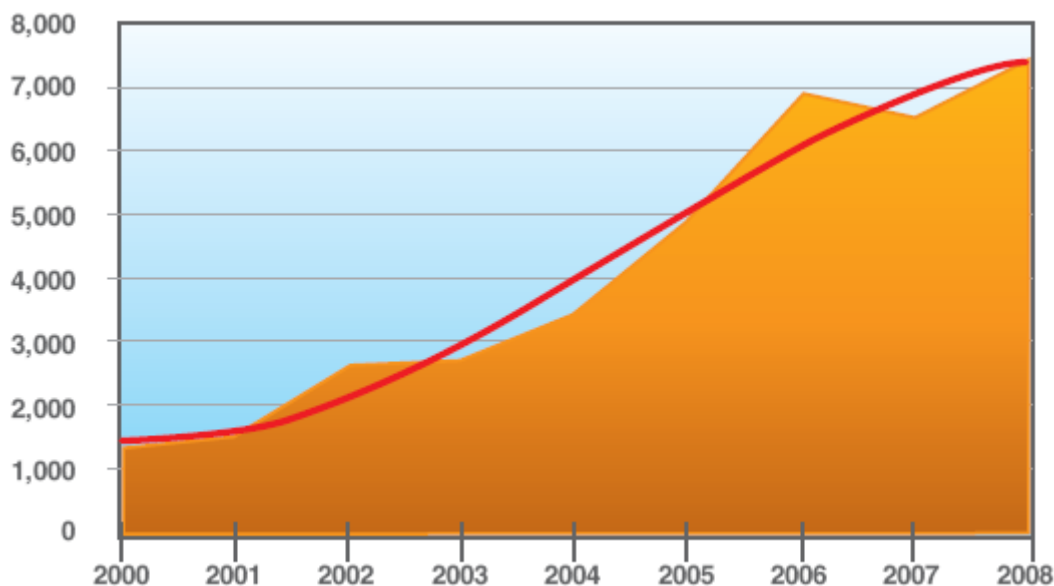


Figura 8: Descobertas de Vulnerabilidades, 2000 – 2008

Para evitar qualquer ambiguidade relacionada à caracterização de vulnerabilidades, a definição da IBM Internet Security Systems (ISS) abaixo é aplicada a este relatório.

Vulnerabilidade – toda a vulnerabilidade, exposição ou definição de configuração relacionada com a informática que possa resultar no enfraquecimento ou na quebra da confidencialidade, integridade ou acessibilidade do sistema de computação.

2008 foi o primeiro ano em que se descobriu um total de mais de 7.000 vulnerabilidades (um aumento de 13,5% em relação a 2007). De 2001 a 2006, o crescimento médio da percentagem anual de descobertas de vulnerabilidades foi da ordem de 36,5%, muito em função do sucesso repentino das vulnerabilidades de aplicativos da Web, da emergência de novas tecnologias da Web, e dos métodos e ferramentas de exploração. De 2006 a 2008, o crescimento caiu para menos de 2% em média.

Embora a introdução de novas tecnologias ou mudanças na adoção de fornecedores de práticas seguras de software deva mudar esta tendência, pelo menos no momento parece que as descobertas de vulnerabilidades chegou a um patamar permanentemente alto.

Tempo para a Descoberta de Vulnerabilidades

Além de registrar os índices anuais mais altos em descobertas de vulnerabilidades, a X-Force também registrou um novo recorde elevado de descobertas mensais, junho de 2008, em que 692 vulnerabilidades foram descobertas, substituindo o registro anterior de 679 a partir de maio de 2006. Embora nos meses do verão costume ser revelado o maior número de vulnerabilidades, a semana mais atarefada no que tange a descobertas acontece normalmente perto dos feriados.

Ano	Semana em que mais vulnerabilidades foram descobertas
2000 – 2005	Semana antes do Natal
2006	Semana antes do Dia de Ação de Graças
2007	Verão
2008	Semana antes do Natal

Tabela 1: Semana em que mais vulnerabilidades foram descobertas

Terça continuou a ser o dia da semana em que se observou o maior número de novas vulnerabilidades, uma tendência que teve início em 2005. Em 2008, a X-Force registrou 1.234 vulnerabilidades nas segundas, seguida de 1.548 nas terças. No resto da semana foi observado um declínio gradativo em novas descobertas de vulnerabilidades, enquanto sábado e domingo continuaram a ficar bem abaixo da média semanal.

O salto nas vulnerabilidades da terça pode ser explicado pelo grande número de consultas e correções de vulnerabilidades lançadas pelos fornecedores na segunda terça-feira de cada mês. A Microsoft encabeçou a tendência no 3º trimestre de 2004, divulgando boletins de segurança regularmente na segunda terça-feira de cada mês, e outros fornecedores de grande porte começaram a acompanhar a processar uma série de razões competitivas ou estratégicas. A *Patch Tuesday*, como é normalmente citada nos círculos de segurança, parece manter a terça-feira como o dia mais ocupado da semana, enquanto o grande paradigma atual da descoberta dos fornecedores se mantém verdadeiro.

Descobertas de Vulnerabilidades por Severidade

A X-Force usa diversas metodologias para classificar a severidade das vulnerabilidades. No entanto, para iniciar este relatório anual, apenas o Common Vulnerability Scoring System (CVSS) será usado na comparação das mudanças ano a ano na severidade das vulnerabilidades.

O CVSS é o padrão da indústria para classificar a severidade e o risco das vulnerabilidades com base nas métricas (básica e temporal) e fórmulas. As métricas básicas são compostas de características que, em geral, não mudam com o tempo. Entre as métricas básicas estão o vetor de acesso, a complexidade, a autenticação e a polarização do impacto. As métricas temporais são compostas por características de uma determinada vulnerabilidade que podem e quase sempre mudam com o tempo, além de incluir a capacidade de exploração, o nível de correção e a confiança do relatório.

Vulnerabilidades identificadas como Críticas pelas métricas do CVSS são aquelas instaladas por padrão, roteáveis na rede, que não exigem autenticação para acessar e permitirão que um atacante domine o sistema ou o acesso no nível da raiz.

A Tabela 2 representa o nível de severidade associado com as pontuações básica e temporal do CVSS.

Nível de Pontuação do CVSS	Nível de Severidade
10	Crítico
7.0 – 9.9	Alto
4.0 – 6.9	Médio
0.0 – 3.9	Baixo

Tabela 2: Pontuação do CVSS e Nível de Severidade Correspondente

Para maiores informações sobre o CVSS, veja uma explicação completa sobre o CVSS e suas métricas no Web site First.org em <http://www.first.org/cvss/>.

Pontuação Básica do CVSS

Os percentuais de vulnerabilidade Crítico e Alto continuam amplamente inalterados desde 2007, embora nas vulnerabilidades de 2008 tenha sido observado um aumento na pontuação Básica.

Como indica a Figura 9, apenas cerca de 1% de todas as vulnerabilidades foram classificadas na categoria Crítica em 2008, uma pequena queda em relação a 2007, em que o percentual de vulnerabilidades críticas foi de 2%. Enquanto as vulnerabilidades de nível Crítico sofreram ligeira queda, o percentual Alto de vulnerabilidades cresceu um pouco, indo de 36% em 2007 para 37,6% em 2008.

Crítico	Crítico
High	Alto
Low	Baixo
Medium	Médio

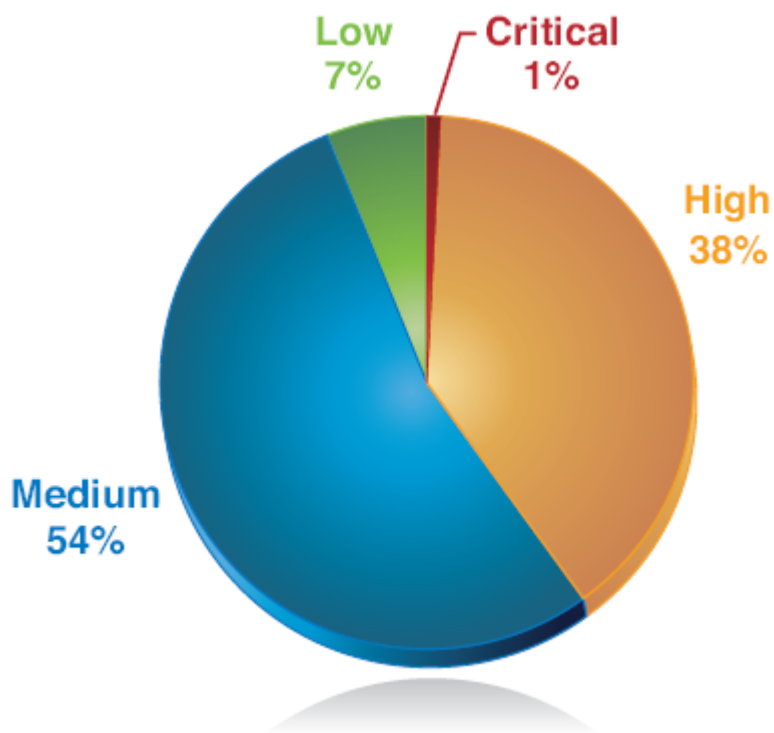


Figura 9: Pontuações Básicas do CVSS , 2008

As vulnerabilidades de nível Médio e Baixo, por outro lado, tiveram um desvio significativo nos percentuais de pontuação básica, que responderam pelo aumento da respectiva severidade de 2008 (Figura 10). Em 2007, 36,7% das vulnerabilidades foram classificadas como Médias, enquanto em 2008, o percentual saltou para 54,0%. As vulnerabilidades de nível Baixo caíram proporcionalmente de 25,4% em 2007 para 7,4% em 2008.

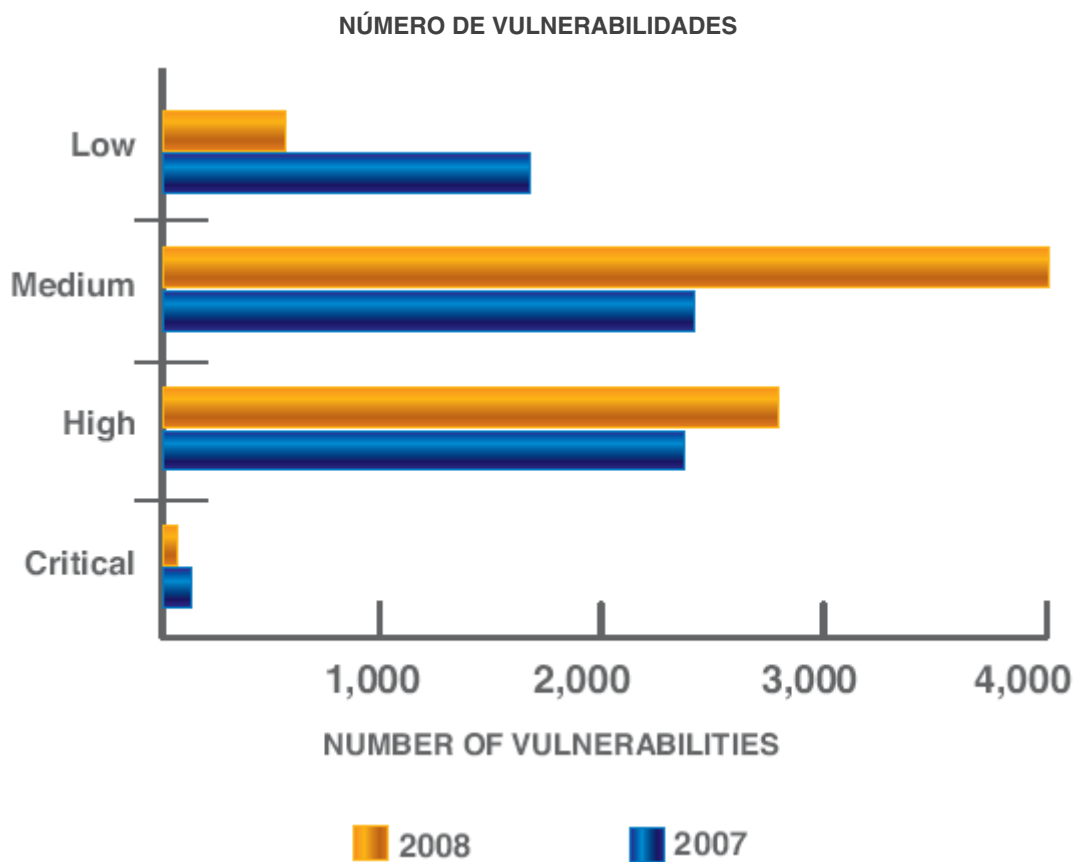


Figura 10: Pontuações Básicas do CVSS, 2007 - 2008

Pontuações Temporais do CVSS

As métricas temporais são compostas por características que se aplicam a uma determinada vulnerabilidade, que podem e quase sempre mudam com o tempo, além de incluir a capacidade de exploração, o nível de correção e a confiança no relatório.

As pontuações temporais, assim como as básicas, também tiveram um aumento global na severidade em 2008 (Figura 11). As vulnerabilidades com pontuação temporal Alta mais do que triplicaram, saltando de 6,5% em 2007 para 21,6% em 2008. As vulnerabilidades de pontuação Média permaneceram basicamente iguais, caindo de 53,1% em 2007 para 49,6% em 2008. As vulnerabilidades com baixa pontuação caíram significativamente, indo de 40,5% em 2007 para 28,9% em 2008.

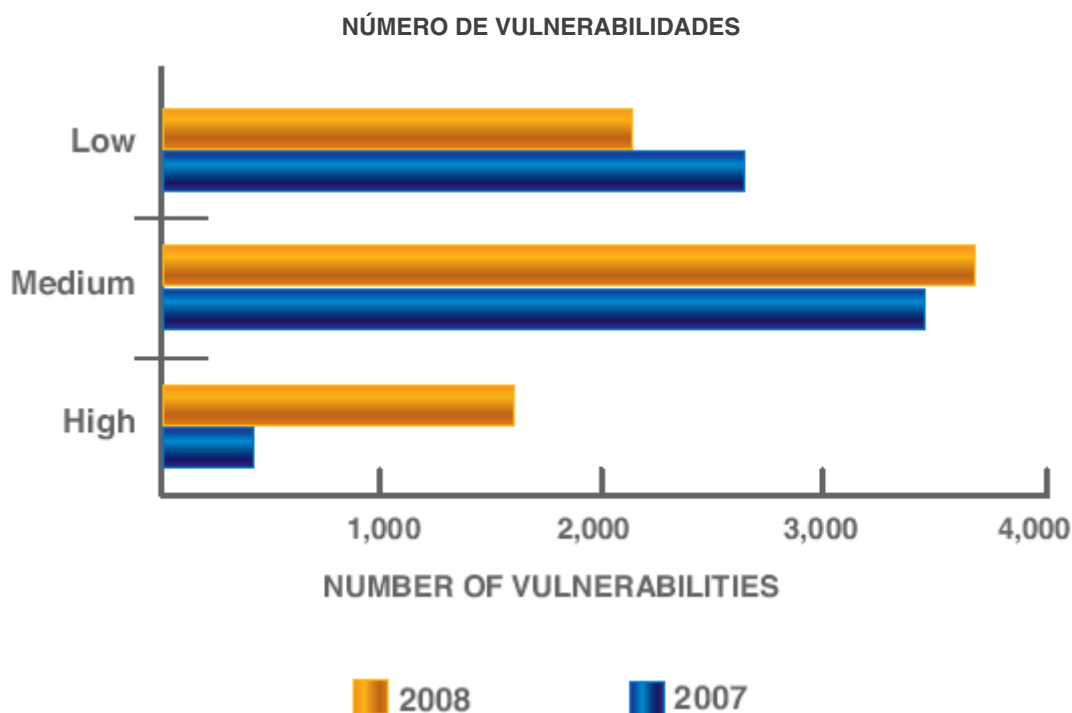


Figura 11: Pontuações Temporais do CVSS, 2007 – 2008

Fornecedores com a Maioria das Descobertas de Vulnerabilidades

As descobertas de vulnerabilidades dos dez principais fornecedores em 2008 responderam por aproximadamente 19,4% de todas as vulnerabilidades reveladas, até um ponto percentual abaixo em 2007. A Tabela 3 revela os dez maiores fornecedores e seus respectivos percentuais de vulnerabilidades em 2008.

Esta estatística não equilibra as descobertas de vulnerabilidades com a fatia de mercado, o número de produtos ou as linhas de código que cada fornecedor produz. Em geral, no software produzido em massa e altamente distribuído ou acessível tende a haver um número maior de descobertas de vulnerabilidades.

Top Ten	Os 10 Maiores
Vendors	Fornecedores
Others	Outros

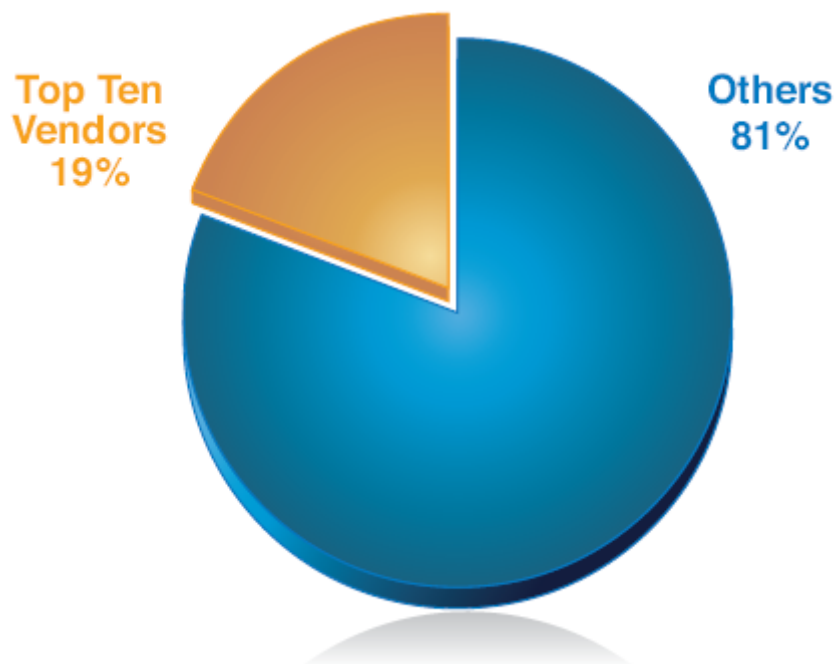


Figura 12: Percentual de Descobertas de Vulnerabilidades Atribuído aos Dez Maiores Fornecedores

Novos Fornecedores na Lista dos Principais

Em 2008, a equipe do banco de dados X-Force incorporou um novo padrão, passando a classificar as vulnerabilidades por fornecedor. Este novo padrão é chamado de CPE, ou Common Platform Enumeration (maiores informações em <http://cpe.mitre.org/>). Esta nova metodologia, mais algumas mudanças na paisagem das vulnerabilidades, trouxe alguns novos fornecedores para a nossa lista dos 10 maiores no relatório da metade do ano de 2008.

o Joomla!, um sistema de gerenciamento de conteúdos de software livre para Web sites

o WordPress, um software para editoração de blogs

o Drupal, outro sistema de gerenciamento de conteúdos de software livre para Web sites

Uma tendência óbvia demonstrada pela figuração destes fornecedores na lista dos 10 maiores é a predominância cada vez maior de vulnerabilidades relacionadas à Web, descritas em detalhes na seção "Vulnerabilidades de Aplicativos da Web", na página 31. Outro ponto comum entre estes três fornecedores é que todos estão escritos em PHP. Se voltarmos às descobertas de 2007 e aplicarmos a nova metodologia CPE às mesmas, vamos descobrir outro novo fornecedor na lista dos cinco maiores, a própria PHP, que seria a quarta classificada na lista dos cinco maiores fornecedores de 2007.

No registro final de 2008, houve uma pequena mudança nesta lista de novos participantes. Joomla! e Drupal permanecem, mas Linux e Wordpress saíram do gráfico. Por pontos, temos:

o TYPO3, outro sistema de gerenciamento de conteúdos open-source para Web sites

o Mozilla, o mais conhecido em função do Mozilla Firefox, um navegador de software livre da Web, que também fabrica outros produtos de software.

O TYPO3 é bem mais similar ao Joomla! e ao Drupal. Todos três são produtos de Web Content Management System (CMS), de plataforma cruzada, software livre e escritos em PHP. Cada um destes produtos permite editoração simples na Web e normalmente interage com bancos de dados no back-end de software livre, como MySQL ou PostgreSQL. Produtos populares e modulares como estes têm bases de códigos desenvolvidos e compartilhados pelos usuários finais. Podemos esperar que o número de vulnerabilidades aumente neste tipo de categoria em correlação com a popularidade e o tamanho da base de código de cada produto.

O Mozilla também é um novo participante quando comparado ao relatório da metade do ano de 2008. No entanto, mais de 70% das vulnerabilidades do Mozilla descobertas em 2008 aconteceram na segunda metade deste ano.

Classificação	Fornecedor	Descobertas
1	Microsoft !	3,16%
2	Apple	3,04%
3	Sun	2,19%
4	Joomla	2,07%
5	IBM	2,00%
6	Oracle	1,65%
7	Mozilla	1,43%
8	Drupal	1,42%
9	Cisco	1,23%
10	TYPO3	1,23%

Tabela 3: Fornecedores com a Maioria das Descobertas de Vulnerabilidades

Correções Disponíveis de Vulnerabilidades

No final de 2008, os fornecedores não haviam disponibilizado correções para resolver 53% de todas as vulnerabilidades descobertas durante o ano. Os fornecedores nem sempre voltam atrás para corrigir as vulnerabilidades do ano anterior. Quarenta e seis por cento das vulnerabilidades de 2006 e 44% das vulnerabilidades de 2007 foram abandonadas, sem que houvesse correção disponível no final de 2008.

No patch at the end of the vulnerability's disclosure year	Sem correção no final do ano em que a vulnerabilidade foi descoberta
No patch at the end of 2008	Sem correção no final de 2008

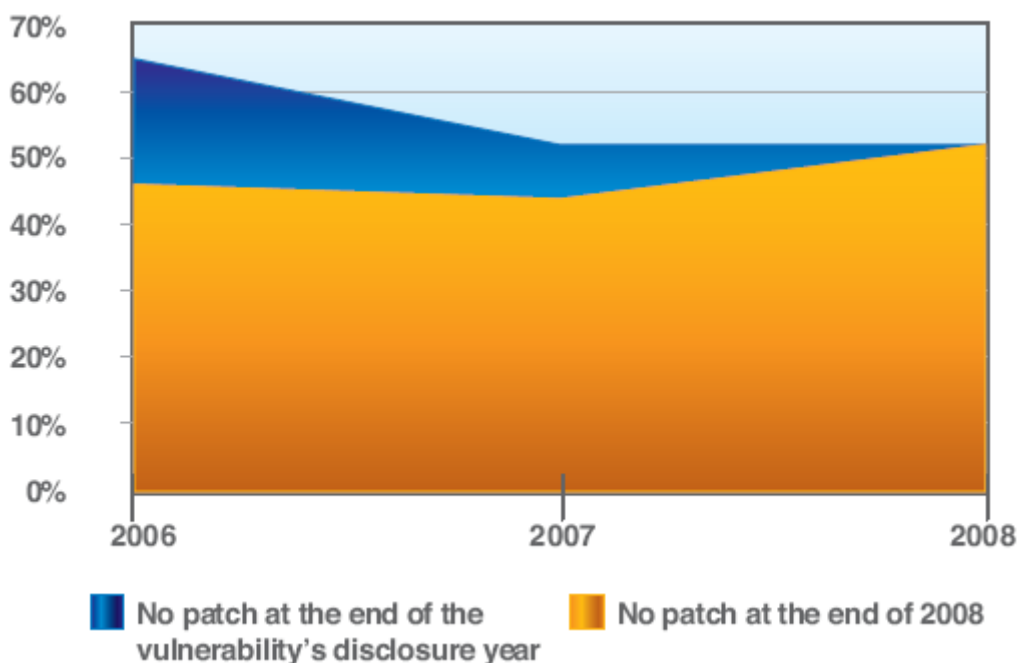


Figura 13: Percentual de Vulnerabilidades Descobertas entre 2006 e 2008, para as quais o Fornecedor Disponibilizou Correção.

Os 10 maiores fornecedores com a maior parte das vulnerabilidades descobertas melhoraram significativamente. Apenas 19% não apresentaram correções, principalmente quando comparados aos demais fornecedores, que deixaram 61% de suas vulnerabilidades sem correção em 2008.

Estes cálculos levaram em conta os fornecedores que reconheceram uma vulnerabilidade publicamente e lançaram a respectiva correção. Não foram considerados os casos em que o fornecedor corrige uma vulnerabilidade em silêncio, sem anunciá-la, ou quando uma correção é lançada por um terceiro.

Vulnerabilidades Exploráveis Remotamente

As vulnerabilidades mais significativas são as que podem ser exploradas à distância, já que não exigem o acesso físico a um sistema vulnerável. As vulnerabilidades remotas podem ser exploradas pela rede ou pela Internet, enquanto as vulnerabilidades locais precisam de acesso direto ao sistema.

O ano de 2008 marca os terceiro ano consecutivo em que o percentual de vulnerabilidades exploráveis à distância atingiu um recorde elevado. Em 2008, elas representavam 90,2% de todas as vulnerabilidades, vindo de 89,4% e 88,4% em 2007 e 2006, respectivamente.

Um fator presente no aumento que ocorreu nos últimos anos é o crescimento do número de vulnerabilidades de aplicativos da Web, que normalmente são exploráveis à distância, e um crescimento contínuo no percentual de sua responsabilidade pelas vulnerabilidades em geral. A Figura 14 mostra o crescimento nas vulnerabilidades exploráveis remotamente ano após ano.

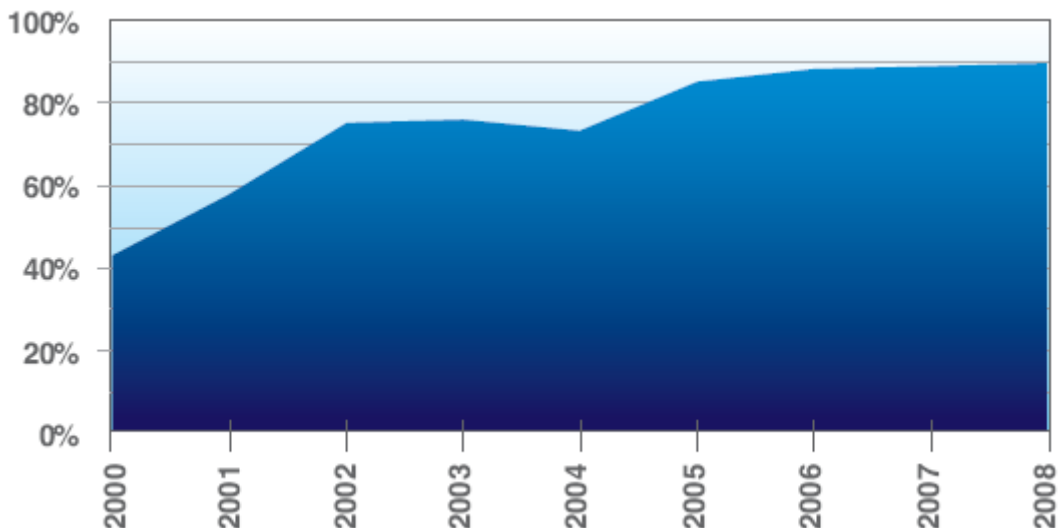


Figura 14: Percentual de Vulnerabilidades Exploráveis à Distância entre 2000 e 2008

Consequências da Exploração

A X-Force categoriza as vulnerabilidades pela consequência da exploração. Esta Consequência é essencialmente o benefício que a exploração da vulnerabilidade oferecer ao atacante. A Tabela 4 descreve cada consequência.

Consequência	Definição
Passagem pela Segurança	Circunda as restrições de segurança como firewall ou Proxy, e o sistema IDS ou um scanner de vírus.
Manipulação de Dados	Manipula dados usados ou armazenados pelo host associados com o serviço ou aplicativo.
Negação de Serviço	Quebra ou rompe um serviço ou sistema para destruir uma rede.
Manipulação de Arquivos	Cria, exclui, lê, modifica ou sobrescreve arquivos
Obtenção de Acesso	Obtém acesso local e remoto. Isto também inclui vulnerabilidades pelas quais um atacante pode executar código ou comandos, porque normalmente permite que o atacante tenha acesso ao sistema.
Obtenção de Privilégios	Podem ser obtidos privilégios somente no sistema local
Obtenção de Informações	Obtém informações como nomes de arquivos e caminhos, código fonte, senhas ou detalhes de configuração do servidor.
Outros	Outros itens não cobertos pelas outras categorias.

Tabela 4: Definições de Consequências das Vulnerabilidades

A consequência primária de exploração de vulnerabilidade mais predominante continua a ser a Obtenção de Acesso, embora tenha havido uma ligeira queda em comparação aos anos anteriores. A obtenção de acesso a um sistema garante ao atacante controle completo sobre o sistema afetado, permitindo o roubo de dados, a manipulação do sistema ou o lançamento de outros ataques a partir daquele sistema. A maior parte dos demais vetores de ataques também permanece similar à dos anos anteriores, com exceção da Manipulação de Dados, que praticamente dobrou e foi atribuída à ascensão das vulnerabilidades de aplicativos da Web com injeção SQL, conforme descrito em "Vulnerabilidades de Aplicativos da Web", na página 31.

Gain Access	Obtenção de Acesso
Data Manipulation	Manipulação de Dados
Denial of Service	Negação de Serviço
Obtain Information	Obtenção de Informações
Bypass Security	Passagem pela Segurança
Gain Privileges	Obtenção de Privilégios
Other	Outros
File Manipulation	Manipulação de Arquivos

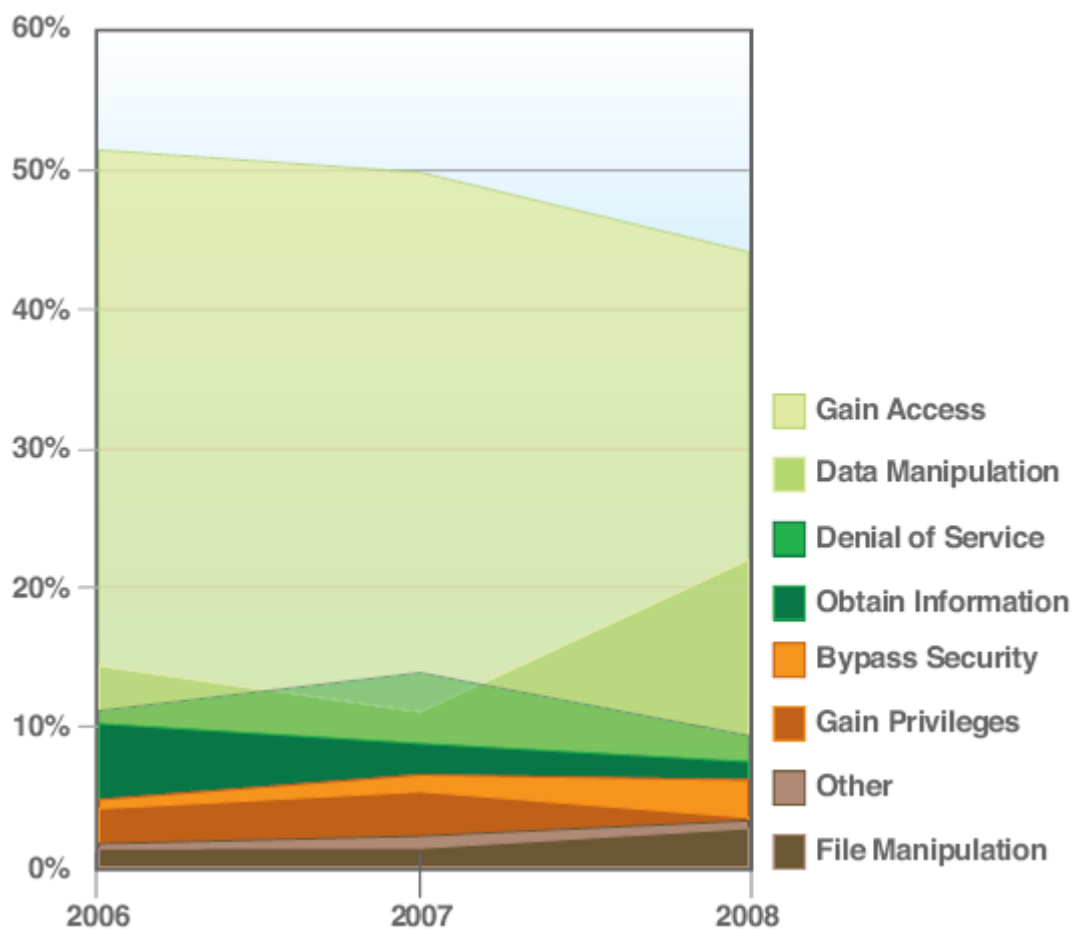


Figura 15: Consequências da Vulnerabilidade como Porcentagem de todas as Descobertas, 2006 – 2008

Vulnerabilidades de Aplicativos da Web

O tipo mais predominante de vulnerabilidade que afeta os servidores hoje em dia é, inquestionavelmente, o relacionado a aplicativos da Web.

A taxa de aumento do número de vulnerabilidades que afetam os aplicativos da Web é estarrecedora. Em 2008, eram da ordem de 54% de todas as descobertas e representavam um dos fatores primários no crescimento geral das vulnerabilidades descobertas durante o ano.

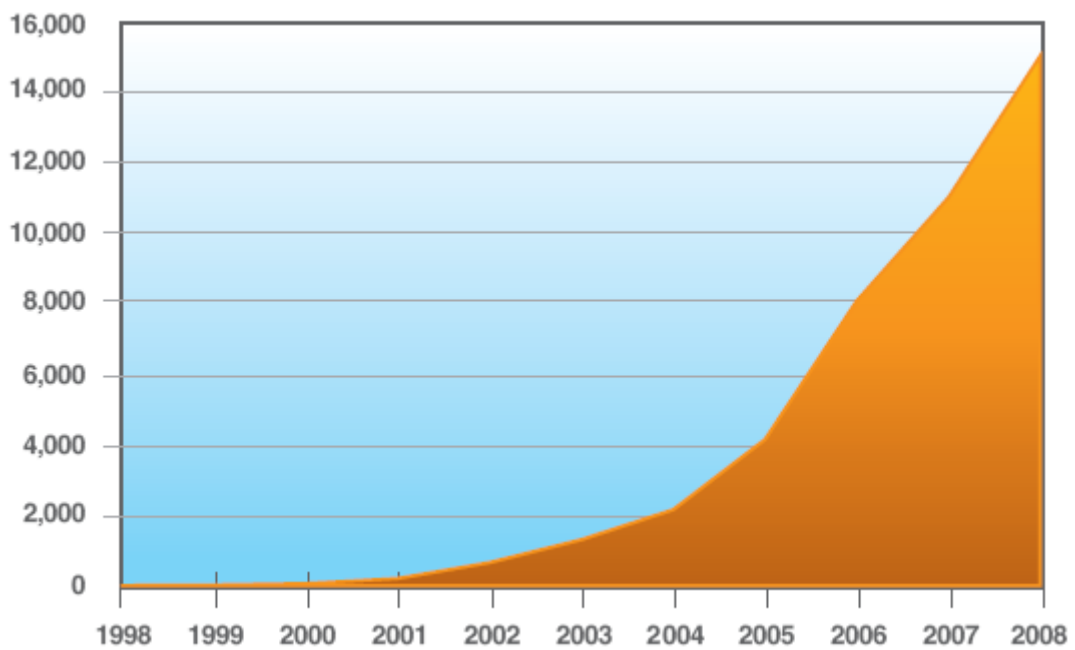


Figura 16: Contagem Cumulativa de Vulnerabilidades de Aplicativos da Web , 1998 - 2008

Aplicativos da Web	54,9%
Outros	45,1%

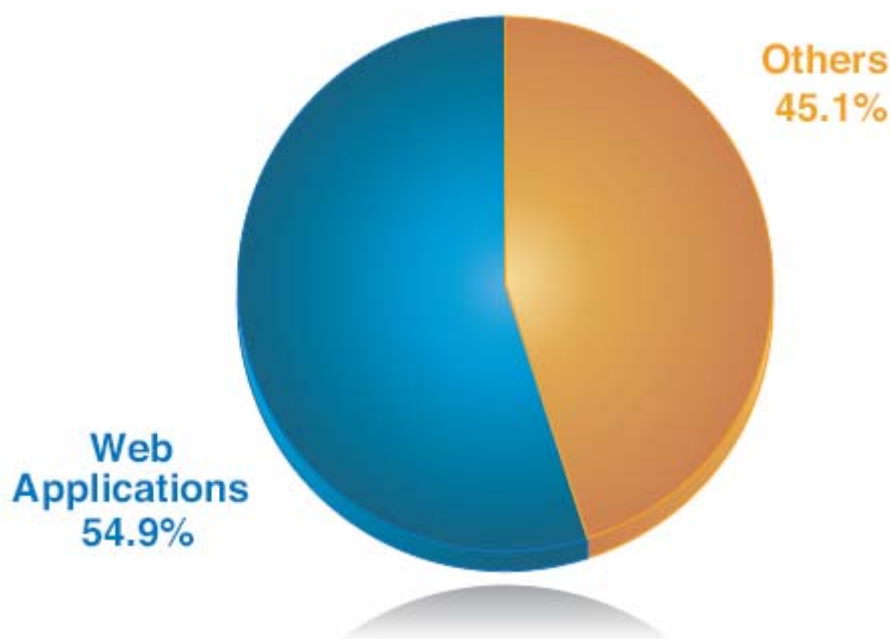


Figura 17: Percentual de Descobertas de Vulnerabilidades de Aplicativos da Web, 2008

Vulnerabilidades de Aplicativos da Web por Categorias de Ataque.

Os tipos predominantes de vulnerabilidades que afetam aplicativos da Web são scripting de sites cruzados (XSS), injeção SQL e arquivos que incluem vulnerabilidades. Em 2008, a injeção SQL substituiu o scripting de sites cruzados como tipo predominante de vulnerabilidade de aplicativo da Web. De fato, o aumento geral de vulnerabilidades de aplicativos da Web em 2008 pode ser atribuído a um enorme pico em vulnerabilidades com injeção SQL, o que superou assustadoramente os 134% de 2007 (Figura 19). Embora os problemas de scripting de sites cruzados sejam também fáceis de descobrir, eles ainda não são tão valiosos para o atacante. Normalmente resultam em furto de cookie, o que permite ao atacante acessar a conta da vítima no Web site vulnerável. A injeção SQL, por outro lado, é quase sempre usada para redirecionar os visitantes de Web sites vulneráveis para o Web site do atacante, onde exploits de execução remota de código podem ser lançados contra o navegador da vítima. Assim, o perfil financeiro da média de vulnerabilidades de scripting de sites cruzados é diferente da média de vulnerabilidades de injeção SQL. O valor de controlar a conta de um usuário num determinado Web site depende do objetivo de utilização do Web site. Por outro lado, ter controle completo do computador do usuário e de potencialmente todas as contas daquele usuário em cada Web site que visita é sempre valioso, independentemente da importância do Web site vulnerável inicial.

Vulnerabilidades de injeção SQL são total e facilmente descobertas. Também é possível usar mecanismos de busca da Web, como o Google, para encontrar sites executando aplicativos vulneráveis, e há muitas ferramentas à disposição do público, que podem verificar a existência da injeção SQL, inclusive alguns plug-ins do Firefox. Não fica imediatamente claro se as vulnerabilidades de injeção SQL aumentaram porque os fornecedores de aplicativos da Web estavam lançando produtos com mais vulnerabilidades, ou se simplesmente havia mais pesquisadores testando a existência de vulnerabilidades, embora provavelmente seja uma combinação das duas coisas. O que fica claro é que os principais fornecedores foram avisados em 2008. Por exemplo, os ataques de injeção SQL contra as tecnologias Microsoft ASP e ASP.NET prepararam a Microsoft para lançar uma consultoria de segurança importante no dia 24 de junho (Microsoft Security Advisory 954462).



Figura 18: Probabilidade de Exploração de Scripting de Sites Cruzados

A Figura 19 mostra como a injeção SQL e outras categorias importantes de vulnerabilidades de aplicativos da Web mudaram com o passar dos anos, e a Tabela 5 descreve cada categoria, inclusive o impacto que elas podem exercer sobre as organizações e sobre os clientes que servem.

Cross-Site Scripting	Scripting de Sites Cruzados
SQL Injection	Injeção SQL
Other	Outros
File Include	Inclusão de Arquivos

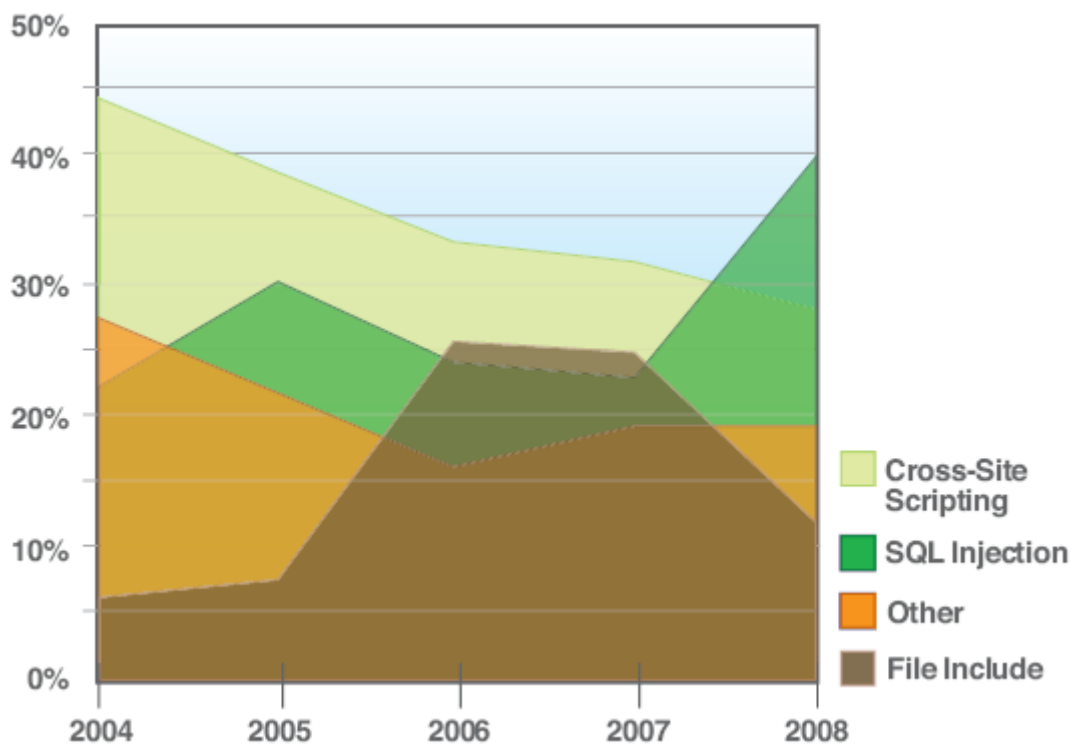


Figura 19: Vulnerabilidades de Aplicativos da Web por Técnica de Ataque, 2004 – 2008

Técnica de Ataque	Descrição
Scripting de Sites Cruzados	<p>Ocorrem vulnerabilidades de scripting de sites cruzados quando os aplicativos da Web não validam adequadamente os dados que o usuário insere nos campos do formulário, a sintaxe das URLs, etc. Estas vulnerabilidades permitem que os atacantes insiram seu próprio script numa página que o usuário está visitando, manipulando o comportamento ou a aparência da página. Estas mudanças na página podem ser usadas para roubar informações sensíveis, manipular o aplicativo da Web de forma maliciosa, ou embutir mais conteúdo na página que explora outras vulnerabilidades.</p> <p>Primeiro o atacante tem que criar um link da Web especialmente fabricado, e depois atrai a vítima para clicar nele (através de spam, fóruns de usuários, etc.) O usuário tende a ser enganado, clicando no link porque o nome do domínio da URL pertence a uma empresa confiável ou familiar. O usuário pode ter a impressão de que tentativa vem da própria organização confiável, e não do atacante, que expôs a vulnerabilidade da organização.</p>
Injeção SQL	<p>As vulnerabilidades de injeção SQL também são relacionadas à validação imprópria de registros do usuário, e elas ocorrem quando este registro (num dos campos do formulário, por exemplo), tem permissão para incluir dinamicamente instruções de SQL que são, então, executadas por um banco de dados. O acesso ao banco de dados do back-end pode permitir que os atacantes leiam, excluam e modifiquem informações sensíveis, e em alguns casos executem códigos arbitrários.</p> <p>Além de expor as informações confidenciais do cliente (como, por exemplo, dados do cartão de crédito), as vulnerabilidades da injeção SQL podem permitir, também, que os atacantes insiram outros ataques no banco de dados, que em seguida podem ser usados contra visitantes do Web site.</p>
Inclusão de Arquivos	<p>As vulnerabilidades de inclusão de arquivos (normalmente encontradas em aplicativos PHP) ocorrem quando o aplicativo recupera o código de uma fonte remota, a ser executado no aplicativo local. No mais das vezes, a autenticidade da fonte remota não é validada, o que possibilita ao atacante o uso do aplicativo da Web para executar remotamente o código malicioso.</p>
Outros	<p>Esta categoria inclui alguns ataques de negação de serviço e técnicas variadas com as quais os atacantes visualizam ou obtêm informações não autorizadas, trocam arquivos, diretórios, informações de usuário ou outros componentes de aplicativos da Web.</p>

Tabela 5: Descrição das Categorias Mais Predominantes de Vulnerabilidades de Aplicativos da Web

Ataques de Exploração ativa e Injeção SQL Automática em 2008.

No passado, a maior parte dos acordos de servidor da Web eram tentativas planejadas de exploração do tipo "uma por vez", que roubam informações ou manipulam um aplicativo de maneira a beneficiar o atacante. Na primeira metade de 2008, a X-Force começou a acompanhar a exploração em massa de Web sites usando ataques de injeção automática de SQL. Em vez de alavancar a injeção SQL para roubar dados, este ataque atualizava os dados de back-end do aplicativo para incluir iFrames que redirecionavam os visitantes a páginas maliciosas da Web. O objetivo destes ataques eram Web sites bastante conhecidos e confiáveis, além de integrarem, também, o kit de ferramentas de exploração ASPROX. Logo depois, o número de ataques e origens de ataques começou a explodir, conforme foi exemplificado pelos dados a seguir, coletados através da monitoração de ataque do ISS Managed Security Services da IBM:

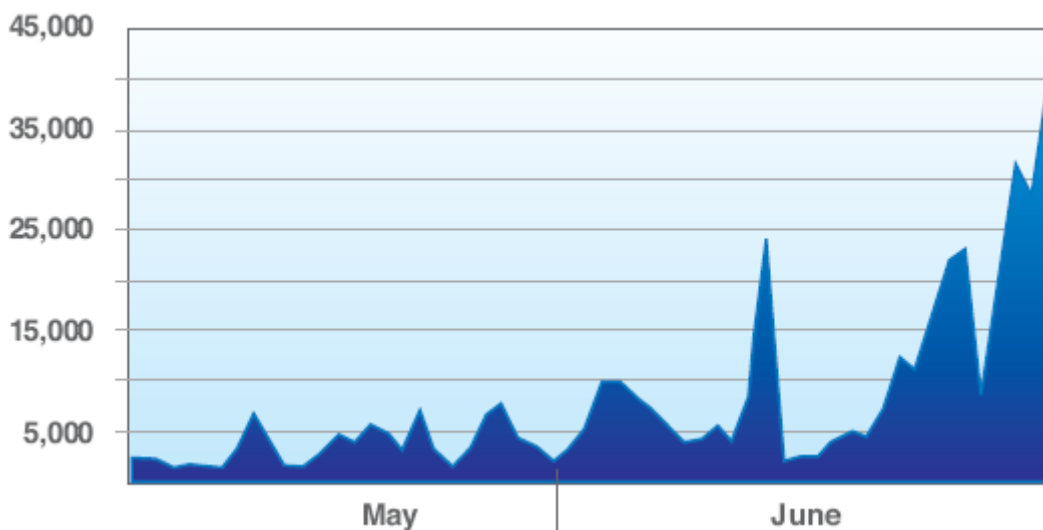


Figura 20: Ataques Iniciais de Injeção SQL Monitorados pelo ISS Managed Security Services da IBM, Maio – Junho de 2008

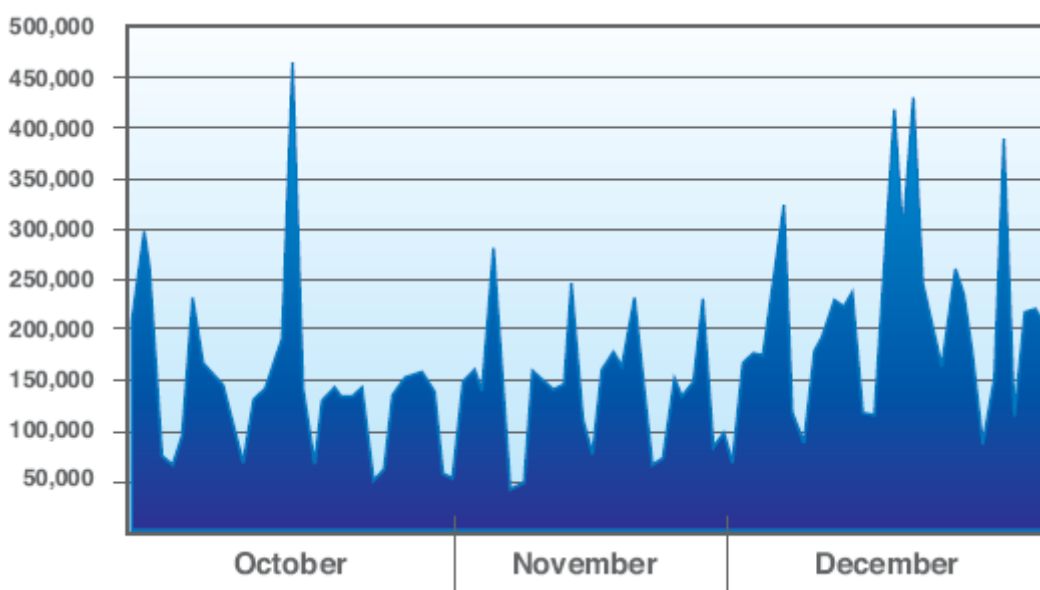


Figura 21: Ataques de Injeção SQL Monitorados pelo ISS Managed Security Services da IBM, 4º trimestre de 2008.

Não há Correção Disponível.

Um número incrível de vulnerabilidades em aplicativos da Web fica sem correção pelo fornecedor do aplicativo para solucionar o problema. No final de 2008 74% de todas as descobertas não tinha correção. Novamente, este número não leva em conta os aplicativos da Web desenvolvidos com exclusividade, que podem não ter passado por testes de vulnerabilidade e talvez nunca cheguem a ver uma descoberta de vulnerabilidade pública para notificar o desenvolvedor de um Web site acerca de questões de vulnerabilidade e exploração potencial.

Não há Correção Disponível	74%
Correções Disponíveis	26%

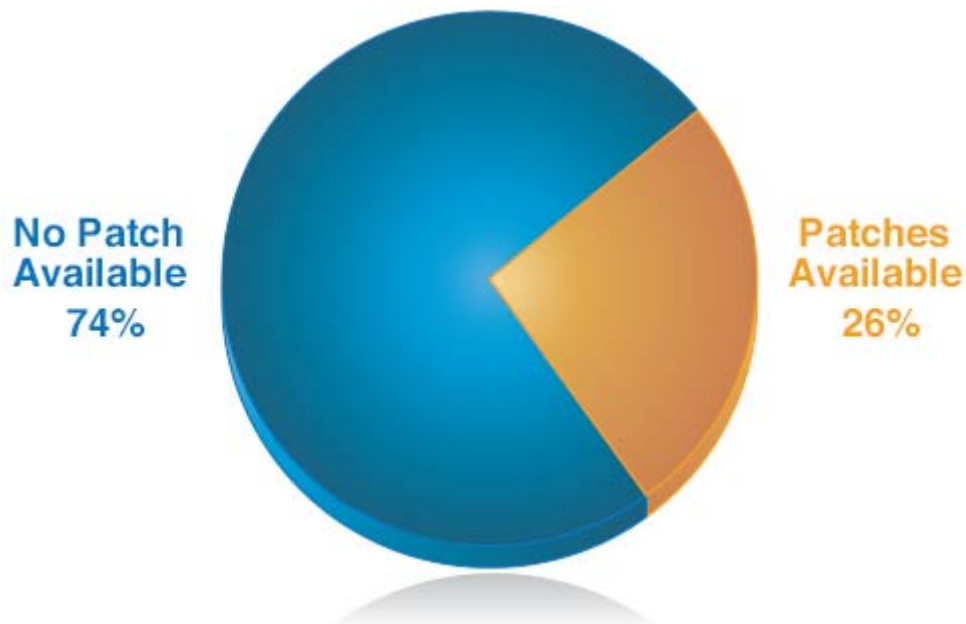


Figura 22: Percentual de Vulnerabilidades de Aplicativos da Web em 2008 sem Correção Disponibilizada pelo Fornecedor no Final de 2008

Web sites Bons Usando Controles de ActiveX Ruins.

Uma prática comum, evidenciada numa análise detalhada de ataques a navegadores da Web, é que muitos Web sites não maliciosos propagam continuamente o uso de controles conhecidos, vulneráveis, de ActiveX. Esta prática tem diversos aspectos negativos. Primeiro, da perspectiva do cliente e do funcionário, o usuário pode ter que instalar o controle de ActiveX vulnerável. Embora existam formas de redirecionar usuários para uma versão corrigida do controle, este redirecionamento não vai funcionar, a não ser que eles estejam executando uma versão atualizada do Internet Explorer ou outro software ativado por ActiveX, que acompanha e bloqueia esses controles vulneráveis conhecidos. Se eles carregarem o controle vulnerável, e depois navegarem para um Web site malicioso que usa um exploit naquele controle, serão explorados sem que o prompt normal lhes pergunte se gostariam de instalar algo novo. Se o controle já estiver lá, eles simplesmente não têm chance.

Da perspectiva da proteção, o uso desses controles vulneráveis conhecidos em Web sites não maliciosos cria uma série de "ruídos" que podem mascarar a atividade maliciosa real.

Relatório de Tendências e Riscos da X-Force® 2008

Página 39

No final de 2008, alguns dos controles ruins de ActiveX encontrados em bons Web sites foram:

Controle de ActiveX	Descrição
Aurigma ImageUploader 4.1	O controle de ActiveX Aurigma ImageUploader 4.1 (ImageUploader4.ocx) é vulnerável a um excesso de buffer baseado na pilha. Referências: CVE-2008-0659 ClassID: F1F51698-7B63-4394-8743-1F4CF1853DE1
BusinessObjects RptViewerAX	O controle de ActiveX BusinessObjects RptViewerAX (RptViewerAX.dll) é vulnerável a um excesso de buffer baseado na pilha. Referências: CVE-2007-6254: ClassID: B20D9D6A-0DEC-4D76-9BEF-175896006B4A
Macrovision InstallShield InstallScript One-Click Install	O controle de ActiveX InstallShield InstallScript One-Click Install pode permitir que um atacante remoto execute um código no sistema. Referências: CVE-2007-5661 ClassID: 53D40FAA-4E21-459F-AA87-E4D97FC3245A
Macrovision InstallShield Update Service Web Agent	O controle de ActiveX Macrovision (isusweb.dll), que foi incluído no InstallShield Update Service, é vulnerável a um excesso de buffer, causado por verificação imprópria de fronteira pela função do DownloadAndExecute(). Referências: CVE-2007-0321 ClassID: E9880553-B8A7-4960-A668-95C68BED571E
Microsoft MDAC RDS Dataspace	O Microsoft Data Access Components (MDAC) pode permitir que um atacante remoto execute um código arbitrário, causado por uma vulnerabilidade no objeto do ActiveX RDS.Dataspace, que faz parte do ActiveX Data Objects (ADO) e foi distribuído no MDAC. Referências: MS06-014/CVE-2006-0003 ClassID: AB9BCEDD-EC7E-47E1-9322-D4A210617116
Microsoft WebViewFolderIcon	O Internet Explorer da Microsoft pode permitir que um atacante remoto execute um código arbitrário no sistema, causado por vulnerabilidade oculta de um inteiro no Windows Shell da Microsoft, que pode ser explorada durante o processamento de um objeto de ActiveX WebViewFolderIcon mal formado com um argumento inválido para o método "setSlice". Referências: MS06-057/CVE-2006-3730 ClassID: 844F4806-E8A8-11D2-9652-00C04FC30871

Tabela 6: Controles Vulneráveis Conhecidos de ActiveX Usados por Web Sites Não Maliciosos

Sistemas Operacionais Mais Vulneráveis.

A X-Force acompanha vulnerabilidades por plataforma e tem produzido métricas este ano para mostrar os sistemas operacionais com as vulnerabilidades mais difundidas. O gráfico a seguir mostra os sistemas operacionais com o maior número de vulnerabilidades documentadas em 2008. Os dez maiores sistemas operacionais acumulam aproximadamente 75% de todas as vulnerabilidades descobertas que afetam sistemas operacionais.

Sistema Operacional	Porcentagem
Apple Mac OS X Server	14,3%
Apple Mac OS X	14,3%
Linux Kernel	10,9%
Sun Solaris	7,3%
Microsoft Windows XP	5,5%
Microsoft Windows 2003 Server	5,2%
Microsoft Windows Vista	5,1%
Microsoft Windows 2000	4,8%
Microsoft Windows 2008	4,1%
IBM AIX	3,7%
Outros	24,9%

Tabela 7: Sistemas Operacionais com a Maioria das Descobertas de Vulnerabilidades, 2008

Diversos sistemas operacionais permaneceram na lista dos cinco maiores nos últimos três anos.

o *Apple Mac OS X*

o *Apple Mac OS X Server*

o *Linux Kernel*

o *Microsoft Windows XP (com uma exceção em 2007)*

Vulnerabilidades e Exploits do lado do Cliente, do Navegador e Outros

As vulnerabilidades que afetam os computadores pessoais formam a segunda maior categoria de descobertas de vulnerabilidades depois das relacionadas a aplicativos da Web e representam cerca de um quinto de todas as vulnerabilidades descobertas.

Vulnerabilidades do lado do cliente: vulnerabilidades que afetam o sistema operacional ou aplicativos em execução nos computadores pessoais. Além do sistema operacional central, componentes vulneráveis podem incluir clientes de e-mail, navegadores da Web, visualizadores de documentos e aplicativos multimídia.

Vulnerabilidades do lado do Cliente – Os Navegadores estão Melhorando

O número global de descobertas de vulnerabilidades que afetam computadores pessoais caiu em 2008, o que pode ser atribuído a algumas das principais categorias. Os dois maiores contribuintes para o declínio estão descritos na tabela a seguir.

Categoria	Declínio Global	
Navegadores e plug-ins de navegadores	10%	Mantido constante (cerca de 300 descobertas tanto em 2007 quanto em 2008)
Cientes de VOIP	49%	Aumentou – quase dobrou o número de descobertas em 2007

Tabela 8: Principais Categorias de Vulnerabilidade Relacionadas ao Declínio Global nas Vulnerabilidades do Lado do Cliente Descobertas em 2008

Relatório de Tendências e Riscos da X-Force® 2008

Página 42

Apesar da queda dos números globais, diversas categorias de vulnerabilidades apresentaram aumentos significativos. O aumento mais marcante estava relacionado ao Java, embora seja importante observar que as vulnerabilidades do Java representam apenas 4% de todas as descobertas de vulnerabilidades do lado do cliente.

o Leitoras e editoras de documentos, subiram 162%. Estes aplicativos também apresentaram descobertas muito mais críticas e altas, com aumento de 168%.

o Aplicativos multimídia, subiram 127%.

Categoria	Aumento Global	Mudança nas Vulnerabilidades de Nível Crítico e Alto
Java	264%	Manteve-se constante
Leitoras e Editoras de Documentos	162%	Aumentou – 168% em 2007
Multimídia	127%	Diminuiu – Cerca de metade do número relatado em 2007

Tabela 9: Categorias de Vulnerabilidades do Lado do Cliente que Apresentaram Aumentos Significativos em 2008

Descobertas de Vulnerabilidades de Nível Crítico e Alto em Aplicativos Predominantes

Conforme descrito em "Economia da Exploração": O que não aconteceu em 2008 e por que, na página 5, dois fatores que podem afetar a probabilidade de exploração maciça incluem o benefício derivado da exploração do alvo (vulnerabilidades de nível crítico e alto) e a predominância dos alvos a explorar.

Determinadas categorias de vulnerabilidades que afetam clientes são discutivelmente mais difundidas do que outras. Por exemplo, embora um percentual significativo de vulnerabilidades esteja relacionado a software de VOIP, esta categoria de software não é nem de longe tão difundida quanto a dos sistemas operacionais, navegadores, aplicativos multimídia, etc.

A Figura 23 mostra as mudanças em descobertas de vulnerabilidades de nível crítico e alto para estes tipos de aplicativos. Apesar do declínio em número com relação a 2007, as vulnerabilidades relacionadas ao navegador ainda estão superando o mais alto percentual de vulnerabilidades de nível crítico e alto que afetam computadores pessoais em 2008 (52% de todas as de nível crítico e alto). Em 6%, os aplicativos de multimídia ainda representam uma parte significativa de vulnerabilidades críticas e altas, embora eles tenham ficado abaixo de 10% em 2007. As vulnerabilidades de sistema operacional de nível crítico e alto ainda estão em declínio. Provavelmente a mudança mais interessante em termos de categoria é o de Leitoras e Editoras de Documentos. Esta categoria contém vulnerabilidades descobertas em aplicativos predominantes como o Microsoft Office e o Adobe Acrobat, entre outros. Estes aplicativos representam 13% de todas as descobertas do lado do cliente de nível crítico e alto em 2008, em comparação com apenas 7% em 2007. Esta mudança está refletida na exploração pública nestes tipos de vulnerabilidades que a X-Force monitorou durante o ano inteiro. Veja “Alvos de Exploração: do Sistema Operacional ao Navegador e Além”, na página 47, para maiores detalhes.

Browser	Navegador
OS	Sistema Operacional (OS)
Security	Segurança
Document Reader or Editor	Leitora e Editora de Documentos

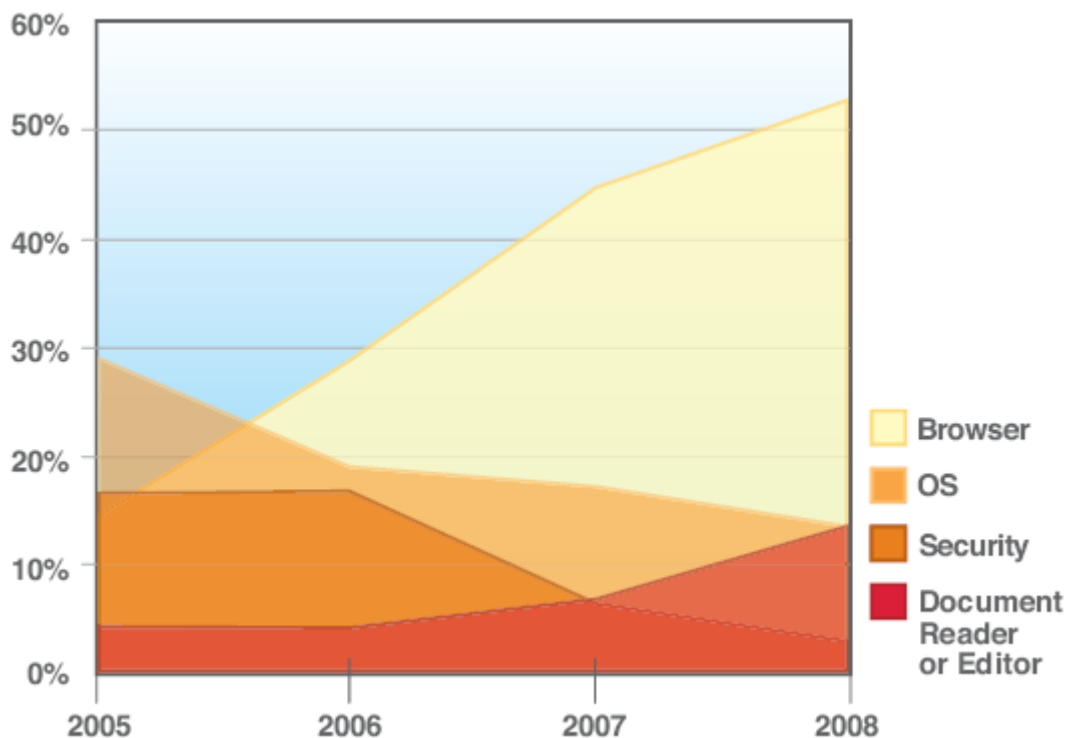


Figura 23: Descobertas de Vulnerabilidades de Nível Crítico e Alto que Afetam Aplicativos do Lado do Cliente por Categoria de Aplicativo, 2005 – 2008.

Vulnerabilidades de Navegador e Plug-in – Queda nas Descobertas do ActiveX

A maior categoria de vulnerabilidades do lado do cliente é a do navegador. Esta categoria inclui não apenas os próprios navegadores, como também uma miríade de plug-ins que neles podem ser instalados. O componente mais afetado de todos os navegadores e tipos de plug-ins é o controle do ActiveX, eterno invasor que representou 46% de todas as descobertas relacionadas a navegador em 2008 e 66% de todas as vulnerabilidades relacionadas a navegador de nível crítico e alto, conforme mostra a Figura 24. Mesmo assim, 2008 pode ser o ano da virada nos controles de ActiveX. Em números absolutos, estas descobertas diminuiram pela primeira vez em 2008, o que representou o fator predominante por trás do declínio global em descobertas relacionadas a navegador.

ActiveX	ActiveX
Internet Explorer	Internet Explorer
Multiple Browsers, Other Browsers & Plug-ins	Diversos Navegadores, Outros Navegadores e Plug-ins
Firefox	Firefox

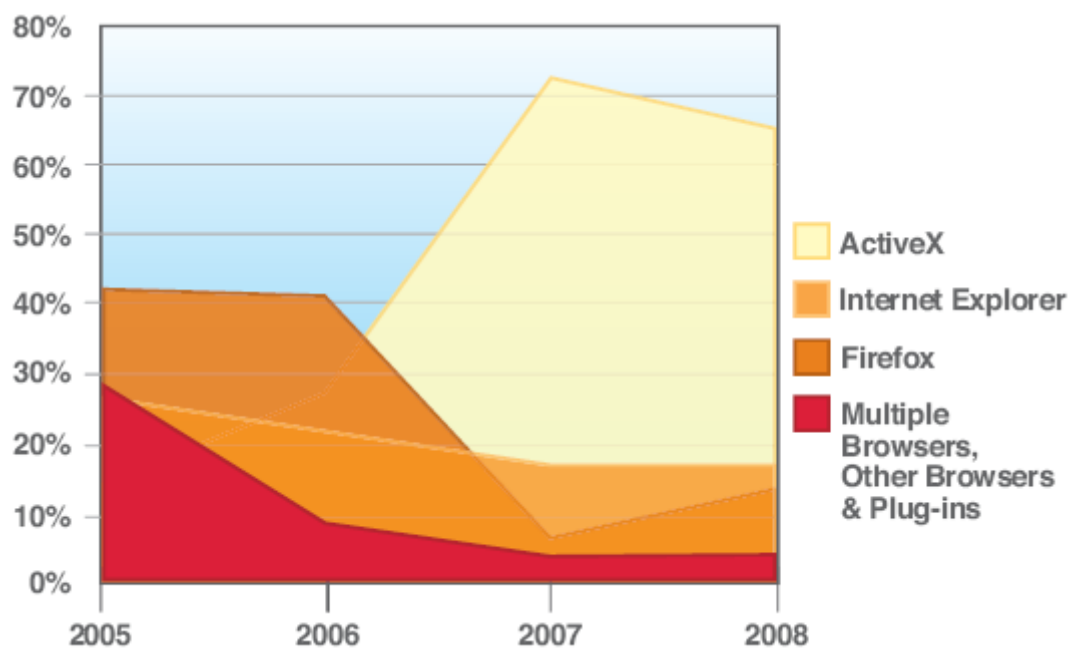


Figura 24: Descobertas de Vulnerabilidades de Nível Crítico e Alto que Afetam Software Relacionado ao Navegador, 2005 - 2008

Infelizmente, a diminuição nas descobertas do ActiveX não parece estar causando impacto sobre a exploração. Assim como ocorre com outras vulnerabilidades relacionadas ao navegador, os atacantes contam com os usuários que não mantêm seus navegadores sempre corrigidos. Embora a Microsoft tenha feito grandes avanços na prevenção da exploração do ActiveX através das mudanças no Internet Explorer, a exploração continua a ser um problema, junto com o uso continuado de controles vulneráveis conhecidos do ActiveX de Web sites não maliciosos (veja "Web Sites Bons que Usam Controles de ActiveX Ruins ", na página 38).

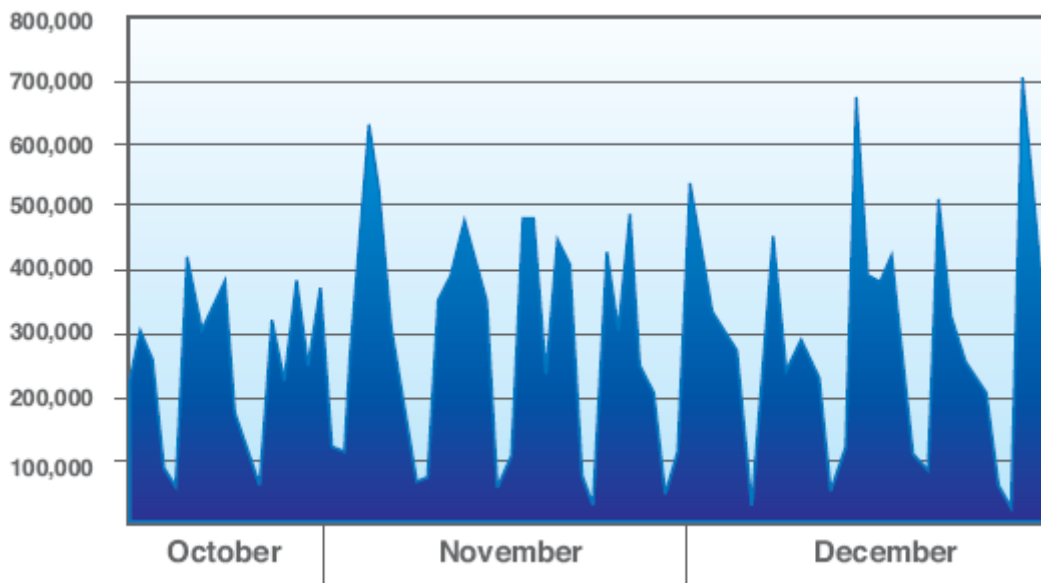


Figura 25: Uso e Exploração de Controle Vulnerável do ActiveX

Disponibilidade do Código de Exploração no Dia Zero

A disponibilidade do código de exploit público, seja a prova de conceito ou totalmente funcional, é um indicador-chave de que uma vulnerabilidade sofrerá exploração ativa. A definição da X-Force de "exploit público" segue o padrão de terminologia do CVSS.

Exploit público: Qualquer código demonstrativo de prova de conceito, parcial ou completamente funcional, ou agente móvel malicioso, como malware, que esteja à disposição do público.

Alguns pesquisadores e organizações de pesquisa publicarão código de prova-de-conceito (PoC) ou detalhes suficientes sobre a vulnerabilidade, para que outra pessoa possa reunir e publicar rapidamente uma PoC. A disponibilidade pública do código de prova-de-conceito aumenta a probabilidade de que a vulnerabilidade enfrentará exploração ao vivo, seja através de tentativas objetivadas ou de um método de distribuição em massa, como num kit de ferramentas de exploit. As ferramentas de teste, como Metasploit e Canvas, são passagens comuns destes exploits públicos.

Nos primeiros anos, podia-se levar semanas ou meses para produzir exploits de prova-de-conceito para descobertas de vulnerabilidades, mas o número de dias entre a descoberta e o exploit público serem divulgados foi significativamente reduzido. Em 2008, 89% desses exploits públicos eram anunciados no mesmo dia ou antes da descoberta oficial da vulnerabilidade. Exploits relacionados ao navegador, em particular, estão cada vez mais propensos à publicação do exploit no mesmo dia. No primeiro semestre de 2008, 94% de todos os códigos de exploit público relacionados ao navegador eram publicados dentro de 24 horas da descoberta oficial da vulnerabilidade, vindo de 79% em 2007. Contudo, no restante de 2008 houve alguma melhora nesta área. Até o final de 2008, apenas 89% de todos os códigos de exploit público relacionados ao navegador eram publicados dentro de 24 horas.

Same Day	Mesmo dia
After Disclosure	Após a descoberta
Before Disclosure	Antes da descoberta

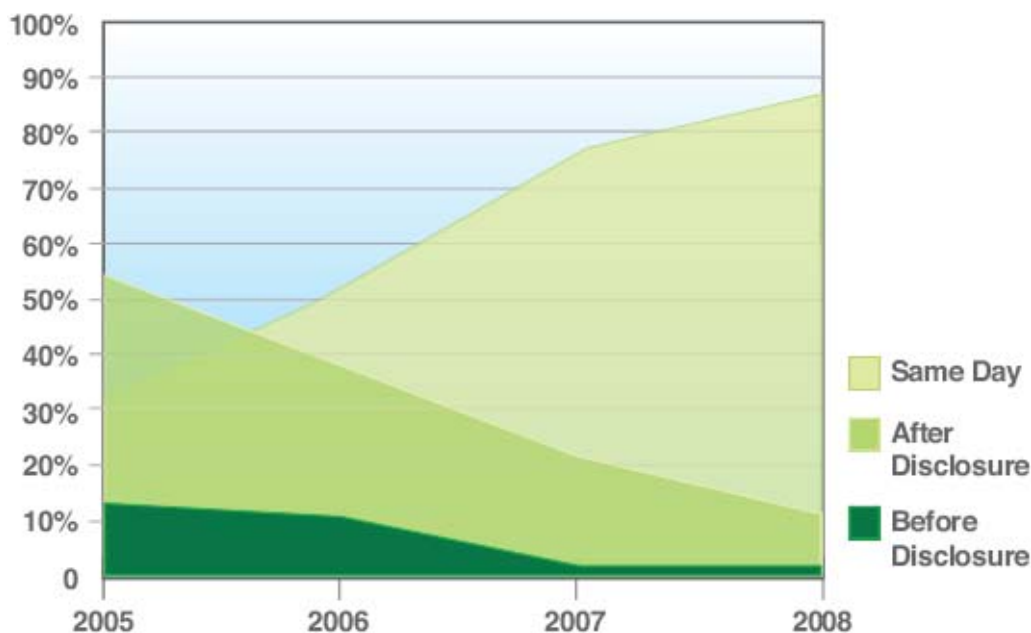


Figura 26: Surgimento de Exploits no Dia Zero

Alvos de Exploit: do Sistema Operacional ao Navegador e Além

Tendências da Exploração do Navegador da Web

A X-Force continua a acompanhar o crescimento da exploração de navegadores da Web através de *crawlers* da Whiro, que combinaram análise independente com os dados de alerta operacional do ISS Managed Security Services da IBM.

A X-Force desenvolveu uma tecnologia especializada em identificar exploits usados, mesmo nos casos mais ofuscados, inclusive onde os kits de ferramentas tentam diversos exploits.

Durante o ano de 2008, ficou claro que a disseminação de exploits solitários de navegadores da Web estava desaparecendo e sendo substituída pelo uso organizado de kits de ferramentas de exploit da Web.

Estes kits de ferramentas podem distribuir todos os exploits de uma vez para visitantes de Web sites, ou pode selecionar exploits específicos com base em dados, como, por exemplo:

- o Conjunto de cookies de navegador pelo kit de ferramentas*
- o Agente de navegador usado pela vítima*
- o Localização geográfica derivada de endereços de IP de vítimas*
- o URL recomendada (a URL que direcionou a vítima ao Web site)*

Relatório de Tendências e Riscos da X-Force® 2008

Página 48

Em muitos casos, estes kits de ferramentas oferecem interfaces de gerenciamento fáceis de usar. As implementações de kits de ferramentas de exploit são, em alguns casos, financeiramente apoiadas por diversos atacantes que recebem créditos por um número de ID associado em suas URLs de ataque, o que é interessante pois permite que os atacantes consigam uma parte da ação com um investimento inicial mínimo. No entanto, não se sabe quantas instalações de kit de ferramenta foram realmente compradas, arrendadas ou pirateadas.

Exploits Mais Populares

Posição	2008 (0 ano inteiro)	2008 2º (Segundo semestre)
1	Microsoft MDAC RDS Dataspace ActiveX (CVE-2006-0003)	Microsoft MDAC RDS Dataspace ActiveX (CVE-2006-0003)
2	RealPlayer IERPCtl ActiveX (CVE-2007-5601)	Microsoft WebViewFolderIcon ActiveX (CVE-2006-3730)
3	Apple QuickTime RSTP URL (CVE-2007-0015)	Internet Explorer "createControlRange" DHTML (CVE-2005-0055)
4	Microsoft WebViewFolderIcon ActiveX (CVE-2006-3730)	RealPlayer IERPCtl ActiveX (CVE-2007-5601)
5	Internet Explorer "createControlRange" DHTML (CVE-2005-0055)	Apple QuickTime RSTP URL (CVE-2007-0015)

Tabela 10: Exploits de Navegador Mais Populares da Web, 2008

Em comparação com o nosso relatório do meio do ano, ainda há quatro dos últimos cinco maiores exploits mais populares de navegadores da Web nos resultados tanto no segundo semestre do ano quanto no ano inteiro. Este tipo de tendência foi observado nos últimos dois anos e na opinião da X-Force, é muito mais em função da conveniência com kits de ferramentas fabricadas em série e piratas. Durante o ano de 2008, a equipe do kit Neosploit anunciou que estava parando; no entanto, foi descoberto mais tarde pela X-Force e outros, que estão sendo usadas cópias atualizadas do Neosploit para disseminá-lo. Em poucas palavras, o Neosploit foi atualizado com diversos novos exploits depois do suposto fechamento.

Relatório de Tendências e Riscos da X-Force® 2008

Página 49

Kits de Ferramenta de Exploit Mais Populares (2º semestre de 2008)

Posição	2008 (O ano inteiro)	2008 2º (Segundo semestre)
1.	mPack (e variáveis)	CuteQQ
2.	CuteQQ	AdM
3.	AdM	mPack (e variáveis)
4.	FirePack	Neosploit
5.	Neosploit	Tornado (e variáveis)

Tabela 11: Kits de Ferramenta de Exploit Mais Populares, 2008

Apesar de muita gente acreditar que os kits de ferramentas de exploit de navegadores da Web são primordialmente distintos, isto não é inteiramente verdade. Em nosso relatório na metade do ano, começamos a discussão da popularidade do kit de ferramentas de exploit em termos que incluíam variáveis. Para manter a perspectiva, podemos relatar um kit de ferramentas como único, como variável, ou como único e variável. Por exemplo, o kit CuteQQ, o mais popular no 2º semestre de 2008, está relacionado ao kit FirePack, que saiu da lista dos cinco maiores. O kit CuteQQ é baseado em outro kit chamado SmartPack que, por sua vez, tomou emprestado elementos do FirePack.

Embora a eclosão do derivativo do Random.JS mPack no início do ano tenha sido responsável por um grande e maciço impulso na popularidade do mPack na época, o estado atual de utilização do mPack é significativamente inferior. Apesar disso, as variáveis do mPack reivindicaram a posição mais alta na nossa lista como o kit de ferramentas de exploit mais popular o ano inteiro.

Outra mudança interessante desde o nosso relatório da metade do ano é que o segundo kit mais popular na lista que publicamos no relatório – cujo nome não era conhecido anteriormente – foi absorvido pela família do kit CuteQQ.

Ofuscamento

Durante o segundo semestre de 2008, a X-Force observou uma redução no ofuscamento e especificamente uma redução no uso de diversas camadas de ofuscamento. As técnicas de ofuscamento normalmente têm sido básicas, como a concatenação da cadeia, bem como *stubs* de decodificador complexos que podem ser, eles próprios produzidos pelo processo de autodecodificação. Recentemente, a X-Force identificou o que pareceu ser uma tendência emergente de camadas múltiplas de autodecodificação. No final de 2008, páginas com script malicioso apresentando autodecodificação normalmente não tinham mais que uma dessas camadas e além disso usavam, predominantemente, concatenação básica de cadeia. Atribuímos as mudanças no ofuscamento de código às alterações nos kits de ferramentas de exploits mais populares. Continuando, é difícil prever se uma redução no ofuscamento vai continuar como uma nova tendência ou se vai se intensificar, novamente.

No relatório do meio do ano, a X-Force comunicou que o uso de Visual Basic Script ou VBScript com exploração de navegador da Web era de 3%. O Visual Basic Script é uma antiga linguagem nativa do navegador Internet Explorer . Outros navegadores, como Firefox, Opera, Chrome e Safari não dão suporte a esta linguagem de script, embora sejam alvo dos atacantes com muito menor frequência devido à fatia de mercado. Durante o segundo semestre de 2008, a utilização do VBScript na exploração de IE aumentou na base de um por site em 562%. Assim, enquanto o VBScript ainda é utilizado por um pequeno número global, seu aumento indica uma provável tendência. Uma explicação possível é que a maior parte das soluções de detecção só dão suporte à análise de JavaScript e isto é, portanto, uma forma de ofuscamento.

Exploração e Ofuscamento de PDF

Durante o ano de 2008, surgiram dois exploits significativos de PDF, implementados durante a disseminação (CVE-2007-5659 e CVE-2008-2992). Embora em termos individuais o número não seja suficiente para entrar na nossa lista das "5 Maiores", sua integração nos kits de ferramentas de exploit ocorreu e é significativa em termos de ofuscamento. As vulnerabilidades estavam no modelo objeto criado pela Acrobat sobre um mecanismo de JavaScript e elas foram, subsequentemente, exploradas desta forma. O JavaScript exploit adotou o mesmo ofuscamento característico, visto nos kits de ferramentas de exploit com *stubs* de decodificador, mas na época os atacantes descobriram que podiam usar o mecanismo DRM com uma senha de documento em branco para criptografar o documento com chaves RC4 de 40 bits ou 128 bits. O sentido desta prática é que descriptografar o documento mesmo com uma chave padrão pode sair caro durante a transmissão e até hoje pode ainda haver software de segurança baseado no host que não é afetado. Noves fora, foi um ano interessante para o ofuscamento de exploit de PDF e muitos, se não a maioria, dos truques para ofuscar ataques foram expostos.

Atividade Global de Ataques do Lado do Cliente

Além do projeto Whiro, a X-Force monitora as tendências de exploração em geral por meio de diversas outras fontes:

o ISS Managed Security Services, responsável pela monitoração de exploits relacionados não apenas a terminais, como também a servidores (inclusive servidores da Web) e infraestrutura de rede em geral. O MSS monitora eventos, cobrindo:

- 7 Centros de Operações de Segurança
- 133 países
- Dispositivos de mais de 15k
- Mais de 2.200 clientes
- 400 milhões de eventos por dia
- 150 milhões de tentativas de intrusão por dia

o Nossa "C-Force," a equipe de pesquisadores que dá suporte aos produtos e tecnologias de ISS Cobion Web-crawling da IBM são os principais contribuintes das seções de distribuição de conteúdos na Web deste relatório

Exploits de Web Sites Maliciosos

Nossa equipe de Content Filtering (Cobion) trabalha com a de Managed Security Services para acompanhar e documentar Web sites maliciosos. O número de URLs maliciosas que hospedam exploits no 4º trimestre respondia sozinho por 50% a mais que o número observado no ano inteiro de 2007. Esta tendência é parcialmente devida à técnica usada por alguns atacantes para definir o mesmo Web site usando muitos nomes diferentes de URL.

Em 2007, o foco dos Web sites que hospedam exploits de clientes estava primariamente dirigido para a exploração de navegadores da Web ou seus plug-ins. Menos de 1% destes Web sites incluíam ataques relacionados a documentos ou aplicativos de multimídia. Em 2008, exploits de multimídia e exploits relacionados a documentos também tinham uma presença mais forte.

Analisando os dados pelo componente afetado temos uma história mais fácil de contar, conforme mostra a Figura 27. Embora o foco da maior parte das explorações esteja sobre a tecnologia ativada pela Microsoft (ActiveX e Internet Explorer), a ascensão na exploração de multimídia e documentos é atribuída ao software da Adobe.

ActiveX	33,8%
Adobe Flash	14,8%
Adobe Acrobat	10,0%
Exploit Genérico ou Ofuscamento	7,1%
Microsoft Internet Explorer	34,0%
Microsoft Windows	0,1%
Mozilla Firefox	0,3%

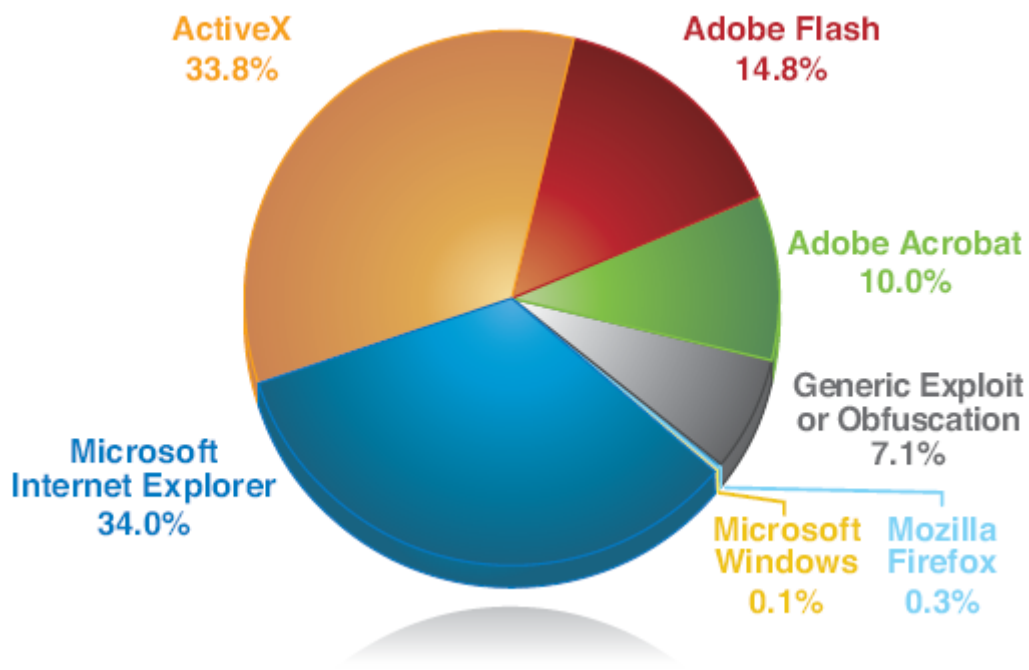


Figura 27: Exploits de Web Sites Maliciosos por Aplicativo Afetado, ISS Cobion Crawler, 4º trimestre de 2008.

Países que Hospedam a Maior Parte dos Web Sites Maliciosos

Além disto, nossos dados mostram que a origem da hospedagem de Web sites maliciosos mudou este ano. Antigamente, os EUA eram os principais hosts de Web Sites maliciosos. Em 2008, a China passou a ser o país que hospeda os Web sites mais maliciosos.

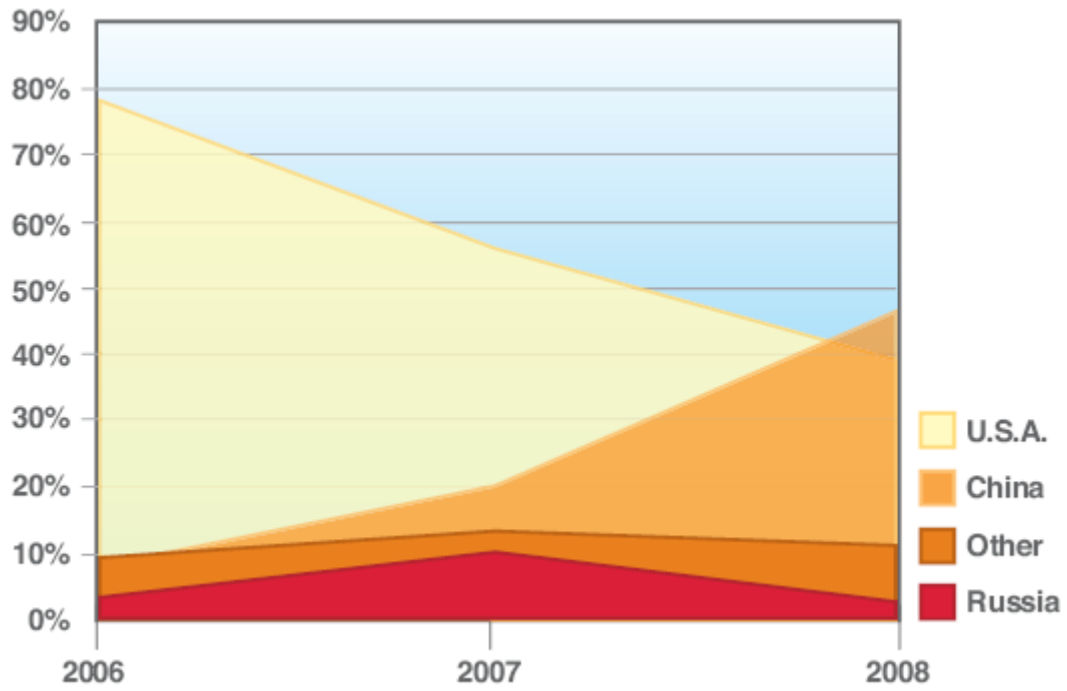


Figura 28: URL Maliciosas por País que as Hospeda, ISS Cobion Crawler, 2006 - 2008

Spam

Os serviços premier de filtragem de conteúdos ISS da IBM oferecem uma visualização de ataques de spam e phishing que abrange o mundo inteiro. Com milhões de endereços de e-mail ativamente monitorados, a X-Force identificou numerosos avanços nas tecnologias de spam e phishing usadas pelos atacantes.

Atualmente o banco de dados de filtragem de spam contém mais de 40 milhões de assinaturas relevantes de spam (cada spam é subdividido em diversas partes lógicas [sentenças, parágrafos, etc.], e uma única assinatura de 128 bits para cada parte) e milhões de URLs de spam. A cada dia há um milhão de assinaturas novas, atualizadas ou excluídas do banco de filtragem de spam.

Os tópicos desta seção são:

o Mudanças no volume de spam, inclusive a remoção da McColo e como isto mudou a distribuição internacional de spam

o Novas tendências rumo a um spam mais simples

o Domínios mais populares usados no spam

o Top Level Domains (TLDs) mais populares usados no spam e por que os top domains são tão populares

o Expectativa de vida de URLs com Spam

o Tendências do país de origem, incluindo páginas da Web com spam¹ (URLs)

o Mudanças no tamanho médio de bites de spam

o Linhas de assunto de spam mais populares

¹A estatística neste relatório no que diz respeito a spam, phishing e URLs usa o IP-to-Country Database fornecido pelo WebHosting.Info (<http://www.webhosting.info>), disponível em <http://ip-to-country.webhosting.info>. A distribuição geográfica foi determinada por solicitação do endereço de IP dos hosts (no caso da distribuição de conteúdo) ou do servidor de correio remetente (no caso de spam e phishing) ao IP-to-Country Database.

Volume de Spam

O volume de spam deste ano não evoluiu e expandiu como nos últimos anos. Em vez de aumentar de forma consistente, o spam se estabilizou próximo ao meio do ano com uma queda significativa em novembro decorrente da remoção da McColo. Depois de aumentar em cerca de 50% de abril a junho, o volume caiu aos níveis de abril em agosto, e em seguida teve uma queda significativa (75%) em novembro. A partir de dezembro, o volume voltou a 70% do nível original.

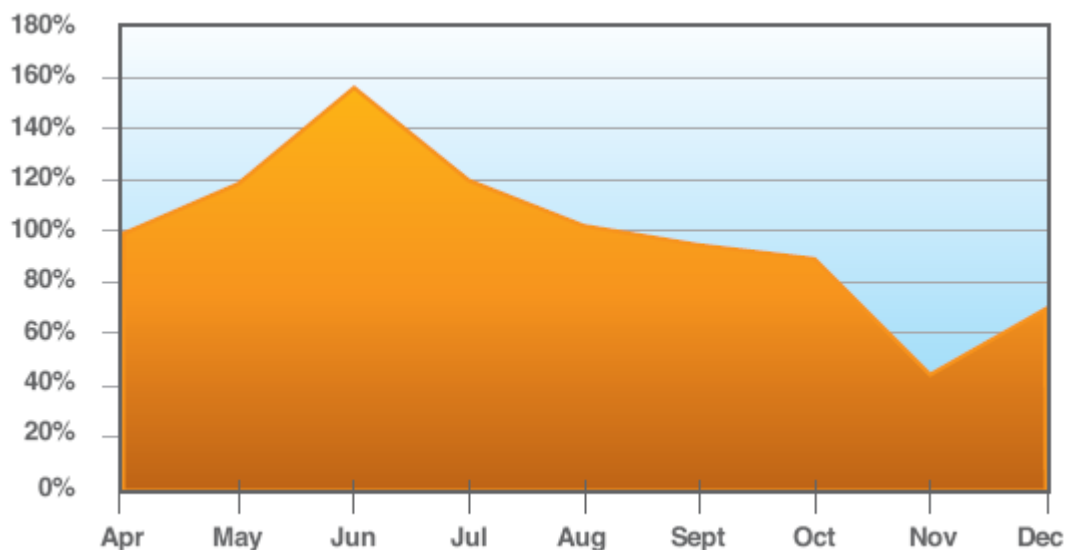


Figura 29: Mudanças no Volume de Spam Desde Abril, 2008

Mais tendências rumo a um spam mais simples

Nos últimos anos houve uma ascensão e agora uma queda, no que a X-Force considera tipos de spam "complexos". O tipo predominante de spam complexo foi originalmente o spam baseado em imagem, mas há muitos tipos de spam que se encaixam na categoria "complexo":

- o Spam baseado em imagem (inclusive imagens complexas com pixels aleatórios, fronteiras aleatórias, ou textos em linhas onduladas)*
- o SPAM em GIF animado*
- o Spam em PDF*
- o Mensagens de spam contendo muito texto aleatório, por exemplo, nos sites de notícias ou poemas*
- o Mensagens de spam contendo estruturas complicadas em HTML que intercalam caracteres aleatórios entre o texto presente no spam*

Spam com URL

No final de 2007, estes tipos complexos de spam começaram a cair e se mantiveram assim em 2008. Portanto, o que os spammers usaram para substituir estes tipos de spam? A Figura 30, que mostra uma elevação no spam de URL (e-mail com spam que contém pouco mais do que um link com um Web site que distribui a mensagem com spam entre as vítimas) e um declínio invertido baseado em imagem pode dar a resposta.

Percentage Image-based Spam	Porcentagem de Spam baseado em Imagens
Percentage URL Spam	Porcentagem de Spam de URL

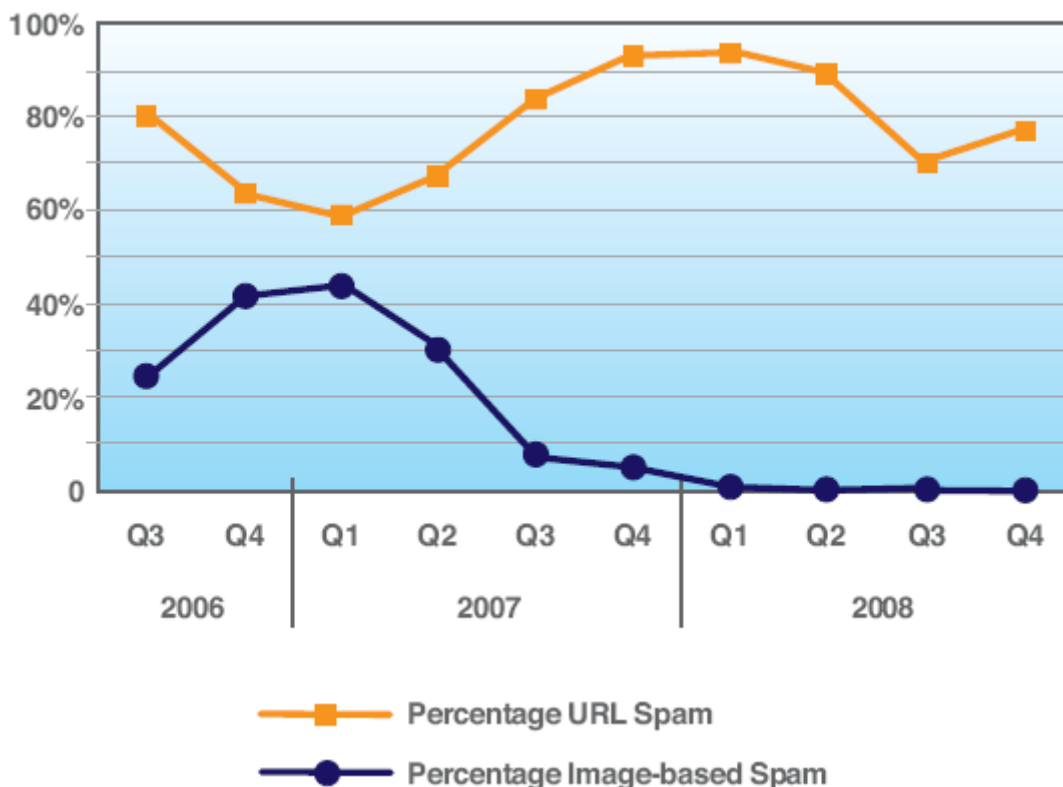


Figura 30: Percentagem de Spam baseado em Image e Spam de URL

Ascensão e Queda de Spam de Texto Simples

A percentagem de spam de texto puro, simples, spam que contém (normalmente) conteúdos de texto puro, curtos, sem HTML ou anexos, cresceu principalmente em paralelo com a percentagem de spam de URL nos dois últimos dois anos e meio. No entanto, no final de 2008, o spam de texto simples começou a cair e, ao mesmo tempo, o spam de URL aumentou.

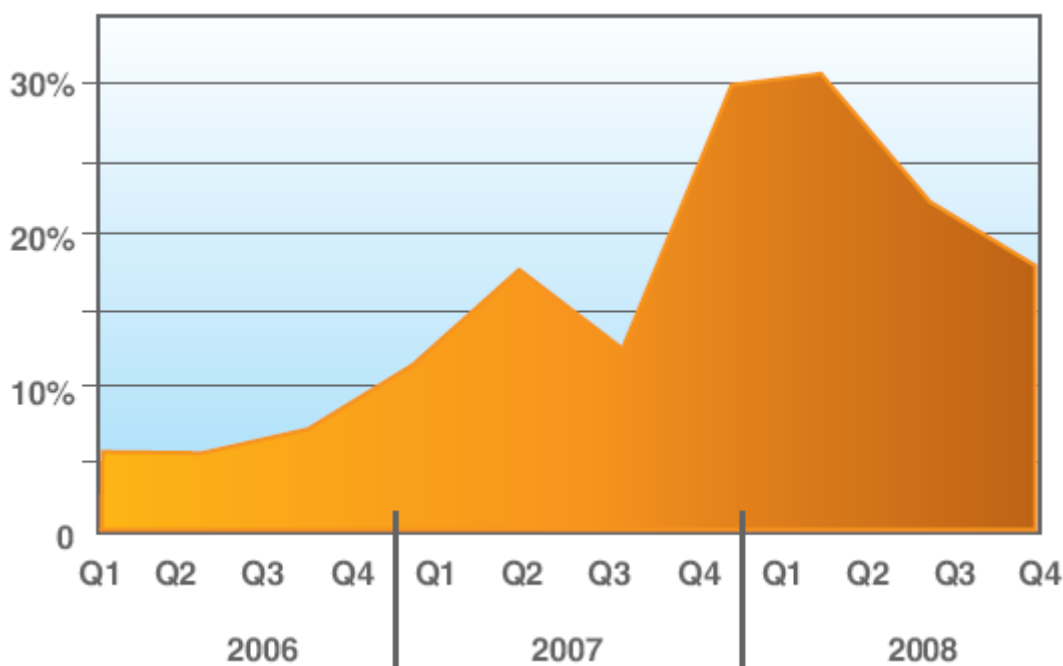


Figura 31: Mudanças na Percentagem de Spam de Texto Simples, Simples

É claro que os spammers começaram a abandonar o spam de texto simples em favor do spam de HTML, possivelmente porque este spam de texto simples está se tornando cada vez mais suspeito e, portanto, menos eficaz. Todos os clientes contemporâneos de e-mail suportam e-mails de HTML, e a maioria dos serviços legítimos de e-mail de marketing e newsletter usa e-mail em HTML mais estimulante em termos visuais em vez de texto simples. Portanto, talvez usar HTML para mensagens de spam crie mais e-mails de aparência legítima, com maior probabilidade de ser eficaz.

O fechamento da McColo também teve um efeito significativo sobre os tipos de spam em circulação. Para maiores detalhes sobre as mudanças no spam durante o fechamento, veja “Remoção da McColo”, na página 72.

Relatório de Tendências e Riscos da X-Force® 2008

Página 58

Domínios Comuns em Spam de URL

Como o spam de URL está aumentando, vale à pena dar uma olhada mais de perto nos nomes de domínio mais frequentemente usados no spam de URL. As tabelas a seguir mostram os dez maiores domínios por mês durante o ano de 2008, destacando alguns domínios-chave.

Posição	Janeiro/2008	Fevereiro/2008	Março/2008	Abril/2008	Mai/2008	Junho/2008
1	livefilestore.com	cnn.net	livefilestore.com	livefilestore.com	live.com	gucci.com
2	smellshort.com	cnn.com	imageshack.us	live.com	tubdyqwenqe.com	notdune.com
3	elementdepend.com	msn.com	beroyal.info	el1te-russ1an-g1rls.com	eurocasinokd.com	hereidea.com
4	opera.com	msnbc.com	forformisskasino.com	myrusfriend.net	stop-fl0p.net	live.com
5	grayany.com	imageshack.us	totalwrite.com	yellowpages.com	bbc.co.uk	heatdark.com
6	creasehappiness.com	reisk.com	cazinoyoumeyou.com	livechatfreex.com	hop-m0p.com	namenot.com
7	msn.com	google.com	casinonewtrip.com	googlegroups.com	t1p-top.com	idolreplicas.com
8	boceph.com	soieuu.com	csinomonster.com	cazinosostermor.com	eurocasinokg.com	davavkos.com
9	alizedup.com	royalfirsteuro.info	beroyal.mobi	777-models-777.com	n1cewomen7.com	vutovlaf.com
10	augsid.com	royalfirsteuro.mobi	beroyal.org	cazinomonste.com	sexymodels123.net	conemain.com

Tabela 13: Domínios Mais Comuns no Spam de URL, 2º Semestre de 2008

Embora a maioria dos spams de URL esteja hospedada em domínios que foram obviamente registradas com esta finalidade, a quantidade de spam de URL que usa nomes de domínios bem conhecidos e confiáveis tem crescido significativamente. No primeiro semestre do ano, estes domínios conhecidos faziam parte da nossa lista mensal dos dez maiores 8 vezes. No segundo semestre do ano, esta contagem superou o dobro, sendo 19 locais preenchidos com nomes bem conhecidos de julho até dezembro. Além de novos nomes aparecerem nos gráficos, surgiu uma nova tendência de usar novos domínios de Web sites, com um grande pico no mês de agosto.

Eis alguns dos Web sites bem conhecidos:

o blogspot.com (editoração de blogs)

o doubleclick.net (desenvolve e oferece serviços de anúncios na Internet)

o google.com (principal mecanismo de busca da Internet)

o googlegroups.com (serviço gratuito do Google em que grupos de pessoas discutem interesses comuns)

o googlepages.com (serviço de criação e hospedagem de Web sites do Google)

o gucci.com (marca da moda italiana famosa no mundo inteiro)

o live.com (um serviço do Windows que facilita a criação de uma página inicial personalizada pelos usuários)

o livefilestore.com (serviço de Web Storage da Microsoft)

o yellowpages.com (diretório telefônico americano)

Novos Web Sites sob a Mira:

o cnn.com (Web site oficial da Cable News Network da Time Warner)

o msn.com e msnbc.com (uma joint-venture entre a NBC Universal e a Microsoft de notícias on-line)

o bbc.co.uk (Web site de notícias on-line da British Broadcasting Corporation)

Relatório de Tendências e Riscos da X-Force® 2008

Página 60

Top Level Domains Comuns em Spam de URL

O Top Level Domain .com domina a tabela de domínios na seção anterior. No entanto, a análise de Top Level Domains revela outra estória sobre o que desperta o interesse dos spammers. As tabelas a seguir mostram os cinco Top Level Domains usados com maior frequência em spams por mês:

Posição	Janeiro de 2008	Fevereiro 2008	Março 2008	Abril de 2008	Mai de 2008	Junho de 2008
1.	com	com	com	com	com	com
2.	cn (China)	cn (China)	net	net	cn (China)	cn (China)
3.	hk (Hong Kong)	hk (Hong Kong)	cn (China)	cn (China)	net	net
4.	net	net	info	biz	info	it (Italy)
5.	info	es (Espanha)	be (Bélgica)	info	tk (Toquelau)	uk (Reino Unido)

Tabela 14: Mais Comuns

Posição	Janeiro de 2008	Fevereiro 2008	Março 2008	Abril de 2008	Mai de 2008	Junho de 2008
1.	com	com	com	com	com	com
2.	cn (China)	cn (China)	cn (China)	cn (China)	cn (China)	cn (China)
3.	net	net	info	net	net	Ru (Rússia)
4.	de (Alemanha)	org	net	biz	es (Espanha)	net
5.	it (Itália)	info	org	org	ru (Rússia)	es (Espanha)

Tabela 15: Top Level Domains Mais Comuns em Spam, 2º Semestre de 2008

Aparte o Top Level Domains genérico (.com, .net, .org, .biz), cada mês revela alguns domínios de nível *top* específicos do país (ccTLDs) que atingem os cinco maiores, os quais são destacados nas tabelas. As tendências específicas do país com o tempo ficam mais evidentes nos gráficos a seguir. A Figura 32 mostra os TLDs com o volume mais alto, e a Figura 33 mostra os participantes da segunda camada. Entre os participantes da camada superior, a China mostrou um aumento significativo até o final do ano.

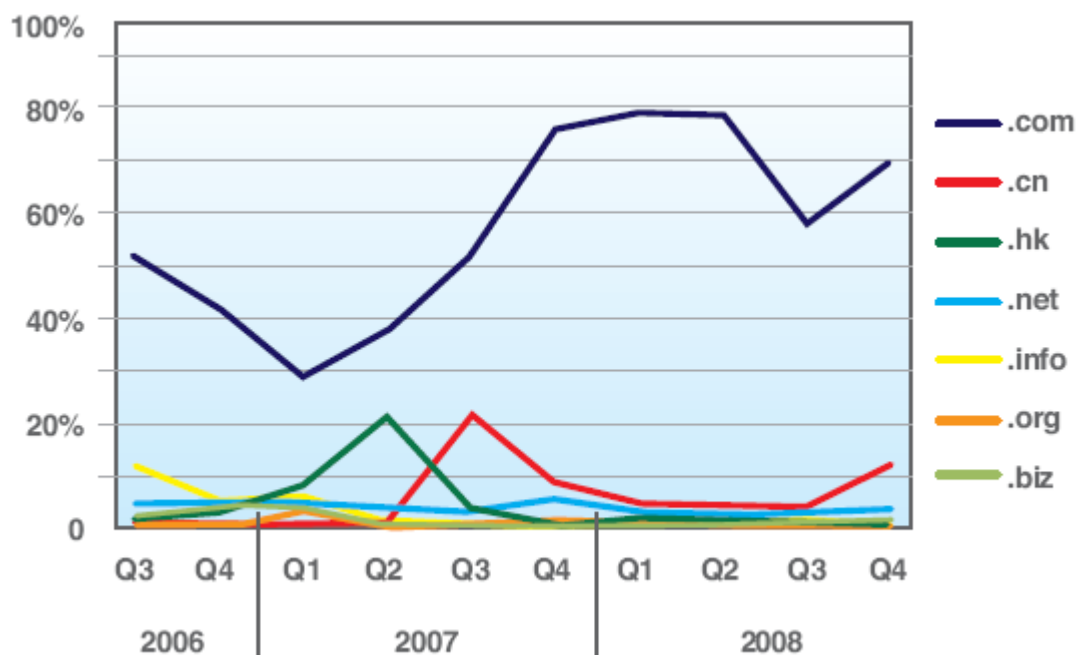


Figura 32: A Percentagem de Spam que Usa URLs de .com, .cn, .hk, .net, .info, .org, .biz

Os Top Level Domains de alguns países atingem, em alguns meses, a segunda liga dos Top Level Domains mais usados. No entanto, ficam bem abaixo do uso de .com e .cn, conforme indicado acima. Mas a variedade de Top Level Domains diferentes usados pelos spammers aumenta:

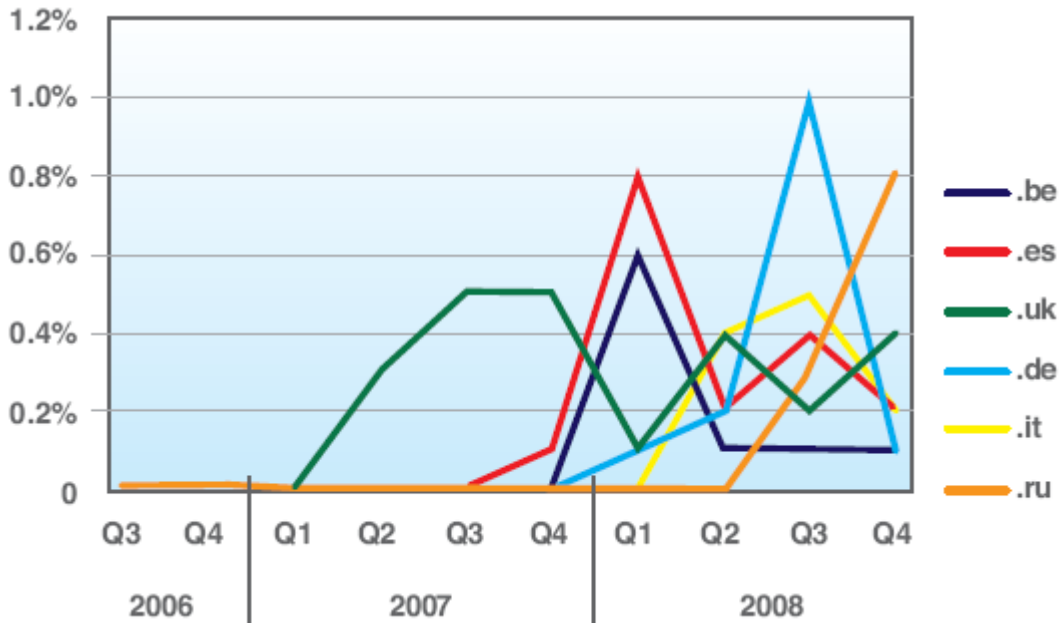


Figura 33: Percentagem de Spam que Usam URLs de .be, .es, .uk, .de, .it, .ru

A maior parte do uso de outros Top Level Domains genéricos ou de código de país fica abaixo de 0,1%.

Por que .com? / Por que .cn?

O uso de URLs .com em spam é o tipo mais insuspeito porque 55% de todos os domínios usados na Internet são .com (fonte: central de dados IBM ISS, veja "Tendências de Conteúdos na Web", na página 87, para maiores detalhes). No entanto, os spammers não usam apenas domínios .com para hospedar seu conteúdo de spam. Eles também usam URLs .com aleatórias que são legítimas nas suas mensagens de spam para fazer com que os filtros de spam legitimem a mensagem em si. Esta tendência se tornou ostensivamente aparente em março de 2008, particularmente, quando observamos quatro vezes a quantidade de novos domínios .com usados em spam, em comparação com os meses anteriores. Numa análise mais profunda, descobrimos que este mês atípico aconteceu em função do uso de domínios .com consistindo de quatro caracteres (como "abcd.com"). Assim, primeiro parecia que os spammers registravam estes nomes de domínios sistematicamente. No entanto, depois de comparar estes domínios com a análise do nosso *crawler* da Web que dá suporte às nossas tecnologias de filtragem da Web, ficou aparente que estes domínios eram registrados anos atrás e foram mantidos como estacionamentos. Os spammers não os registravam. Eles simplesmente os usavam enquanto as URLs de Spam verdadeiras faziam suas mensagens parecerem mais legítimas.

Outro TLD popular era o .cn. Dez por cento de todo o spam continha uma URL .cn no último trimestre de 2008. Uma das razões pode ser o fato de ser econômico e fácil registrar um domínio .cn. Em alguns casos, os spammers e phishers usavam um domínio .com familiar com um TLD .cn em seu lugar. Em comparação com outros TLDs de países, o .cn tem mais facilidade de enganar visualmente usuários insuspeitos (compare "domain.com" com "domain.cn" *versus* "domain.ru"). No entanto, a principal razão de estarmos vendo tantos TLDs .cn é que uma percentagem crescente de spams de URL foi direcionada aos chineses.

Expectativa de Vida de URLs com Spam

Nos últimos anos, a expectativa de vida que as URLs que essas mensagens de spam indicam era cada vez mais curta. Quanto mais rápido elas são descobertas e retiradas, mais probabilidade há de não serem detectadas. Há dois anos e meio, mais da metade das URLs usados em spam ficavam ativos durante mais de um mês. No final de 2008, mais de 97% dessas URLs ficavam ativas no máximo uma semana, conforme indicado na Figura 34. Embora esta tendência dos ciclos de vida se tornarem mais curtos tenha progredido por algum tempo, agora é bem mais relevante com o ataque violento de spams baseados em URL que ocorreu no ano passado.

1 week or less	No máximo 1 semana
Between 1 week & 1 month	Entre 1 semana e 1 mês
Longer than 1 month	Mais de 1 mês

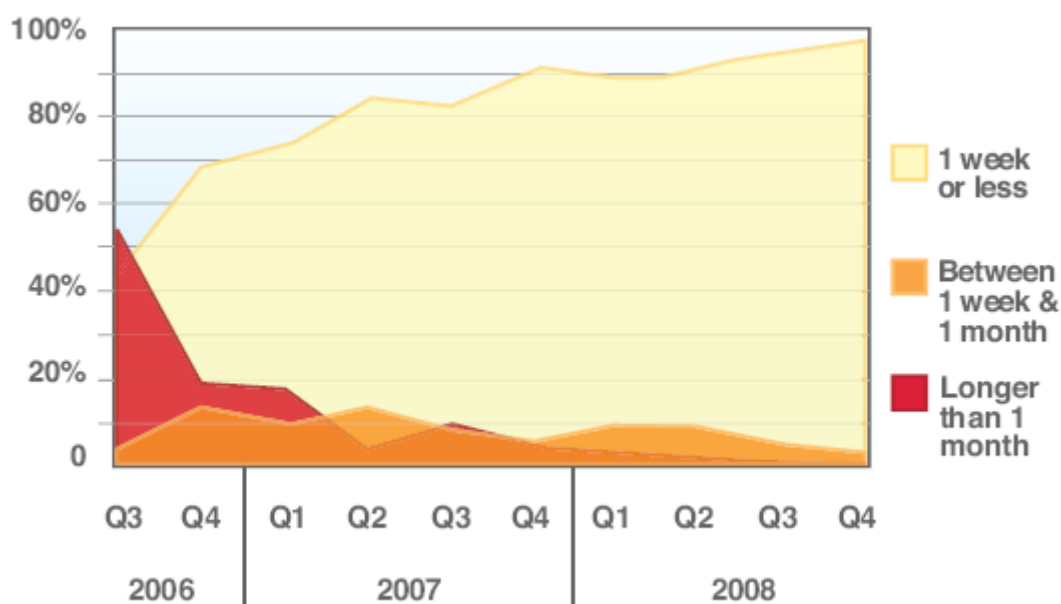


Figura 34: Expectativa de Vida de URLs com Spam

Spam – País de Origem

O mapa a seguir mostra os pontos de origem² de spam em termos globais no ano de 2008. O mapa seguinte mostra o ponto de origem de spam global. Rússia, EUA e Turquia são responsáveis por cerca de 30% do spam do mundo inteiro.

Rússia	12,0%
E.U.A.	9,6%
Turquia	7,8%
Brasil	5,6%
China	4,4%
Coréia do Sul	4,0%
Reino Unido	3,3%
Espanha	3,2%
Polônia	3,2%
Alemanha	3,2%

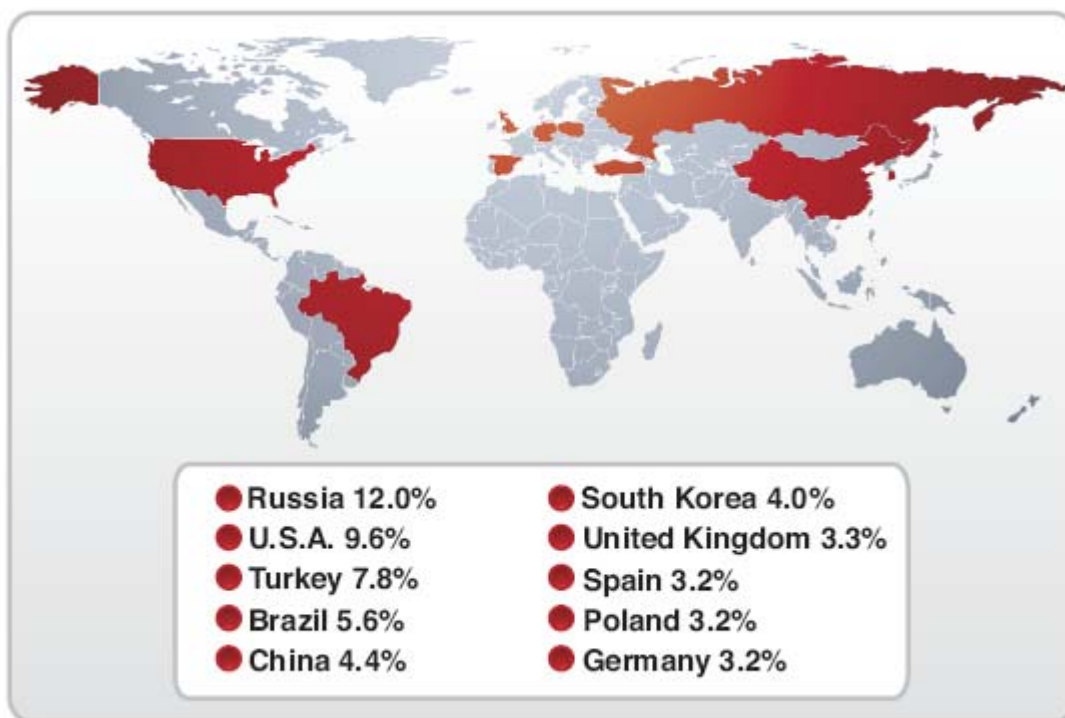


Figura 35: Distribuição Geográfica de Remetentes de Spam

² O país de origem indica a localização do servidor que enviou o e-mail com spam. A X-Force acredita que a maioria dos e-mails com spam é enviada por redes com bot. Como os bots podem ser controlados de qualquer parte, a nacionalidade real dos atacantes por trás de um e-mail de spam pode não ser a mesma do país de origem do spam.

Spam – Tendências do País de Origem

Nos últimos três anos, o número de spams originários de servidores na Rússia, Turquia e Ucrânia aumentou. Além disso, diversos países (Brasil, China e Reino Unido) tiveram um crescimento lento, mas sustentado.

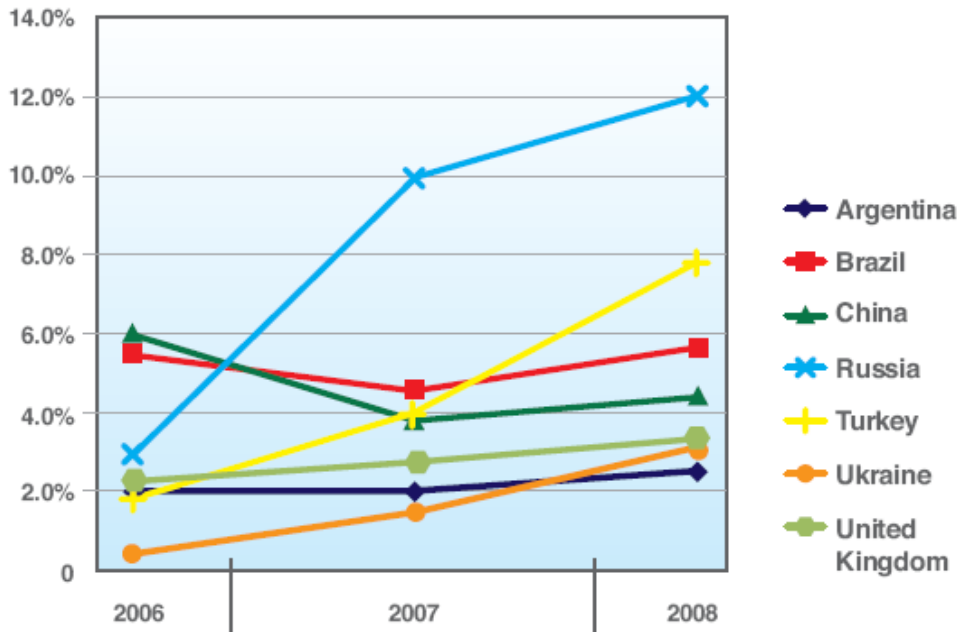


Figura 36: Tendências de Origem de Spam, Ganhadores e Sustentadores de Longo Prazo

Em contraste, diversos países diminuíram, conforme indicado na Figura 37:

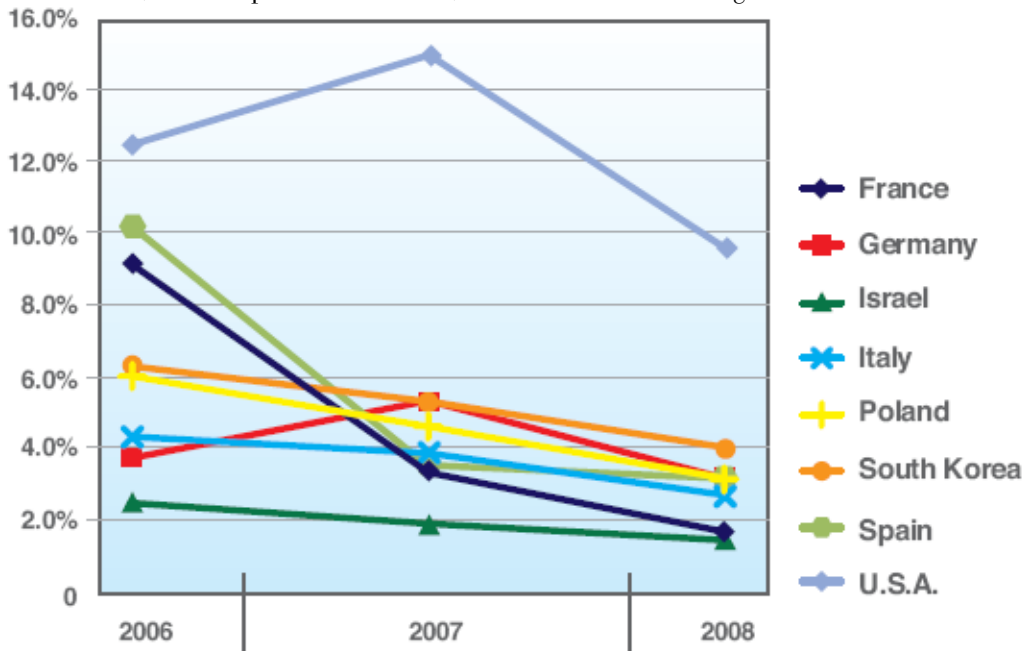


Figura 37: Tendências de Origem de Spam, Declinadores de Longo Prazo

Relatório de Tendências e Riscos da X-Force® 2008

Página 67

URLs com Spam – País de Origem

O mapa a seguir mostra onde estão hospedadas as URLs com spam.

China 20,6%	Coréia do Sul 4,%
E.U.A. 19,4%	Letônia 2,%
Romênia	França 2,%
Hungria 6,%	Argentina 2,%
Rússia 5,%	Polônia 2,%

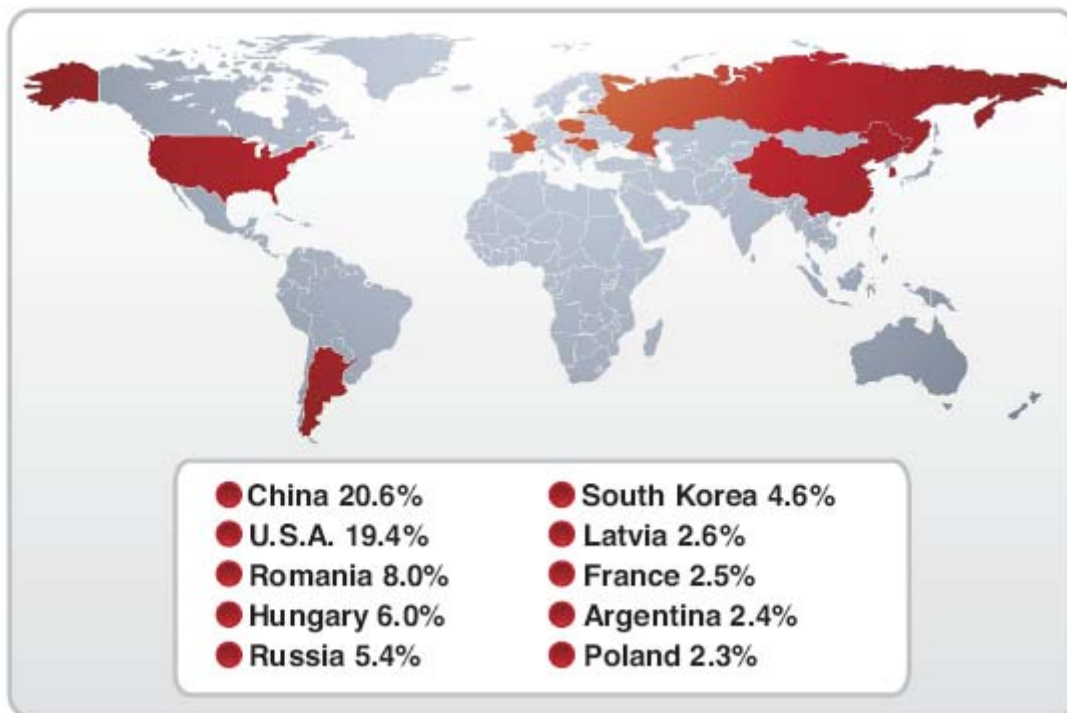


Figura 38: Distribuição Geográfica de URLs com Spam

URLs com Spam – Tendências do País de Origem

Nos últimos três anos, foi possível observar uma tendência de conteúdos de spams hospedados na Rússia e na Romênia, com um declínio na maioria dos outros países. A China e os EUA ainda hospedam a maior parte do conteúdo de spam, conforme indicado na Figura 39. A Figura 40 mostra países que tiveram um aumento gradativo nos últimos anos, e a Figura 41 mostra os países que hospedaram um percentual significativo de URLs com spam no passado, estando agora bem menos ativos.

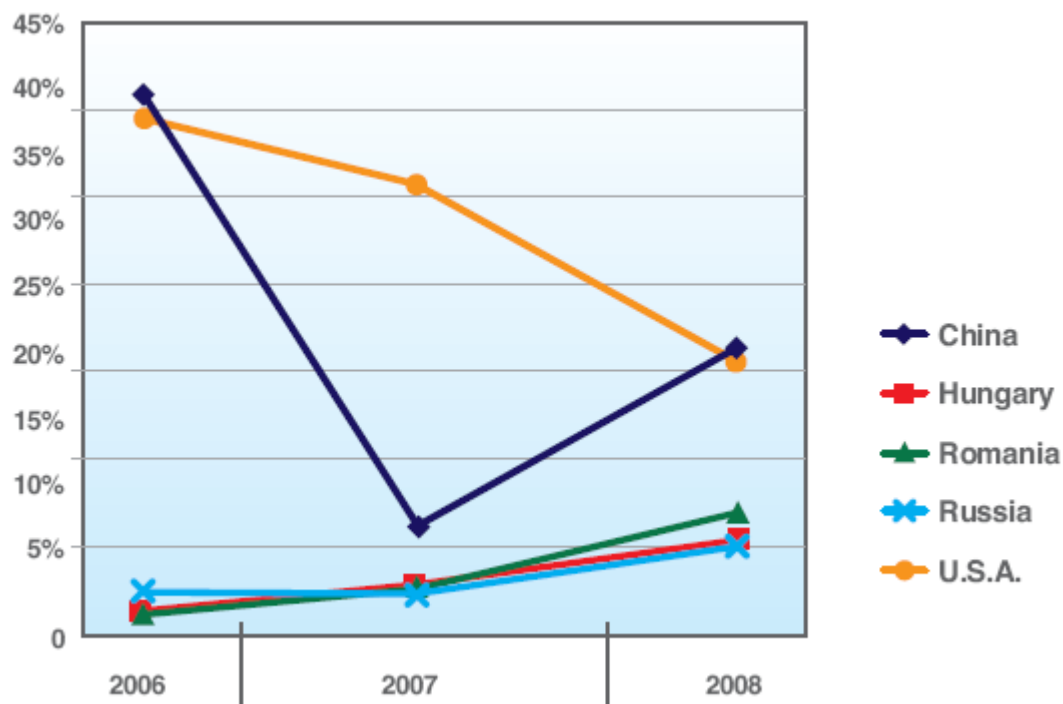


Figura 39: Hosts de URL com Spam, Principais Contribuintes

Relatório de Tendências e Riscos da X-Force® 2008

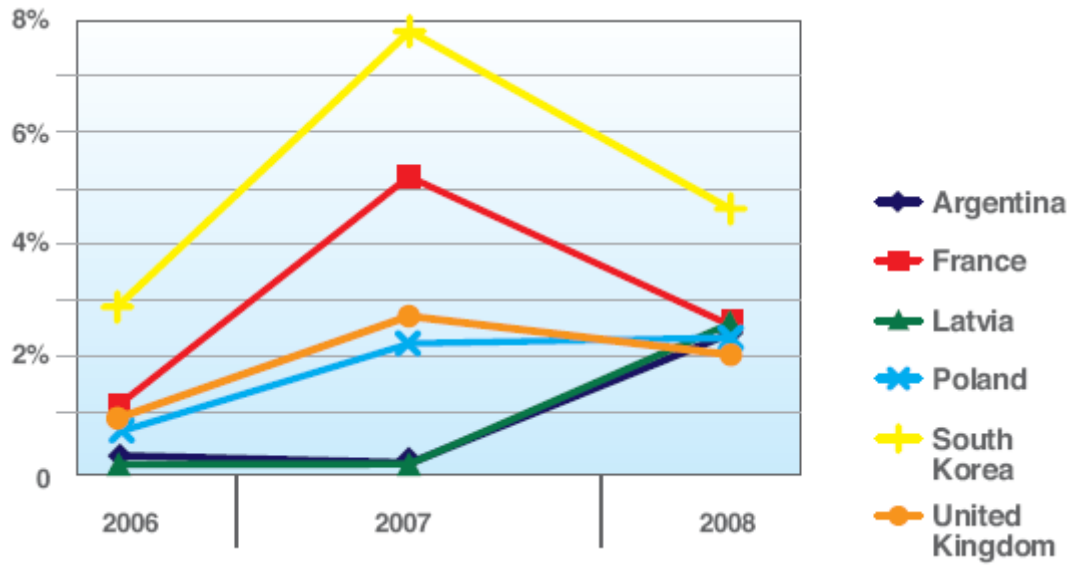


Figura 40: Hosts de URL com Spam, Ganhadores e Sustentadores de Longo Prazo

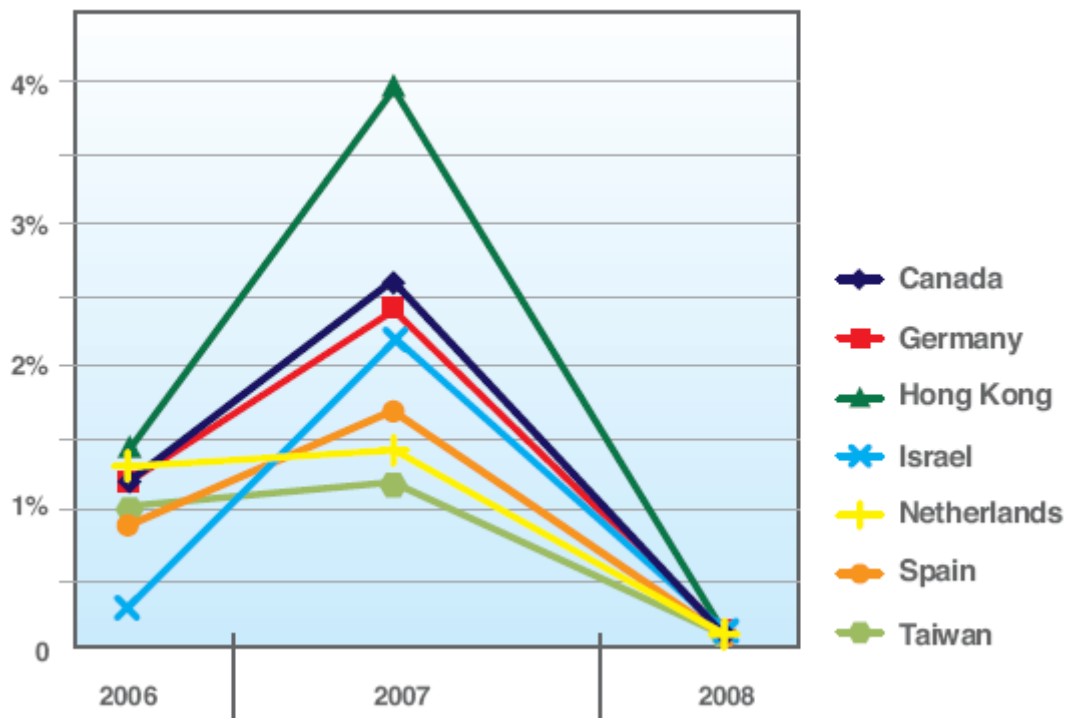


Figura 41: Hosts de URL com Spam, Declinadores a Longo Prazo

Spam – Tamanho Médio de Bytes

A mudança mais significativa no tamanho médio de bytes de Spam ocorreu no final de 2007 e correspondia ao declínio de Spam baseado em imagem. Em 2008, o tamanho de bytes começou a subir ligeiramente até a remoção da McColo no final do ano.

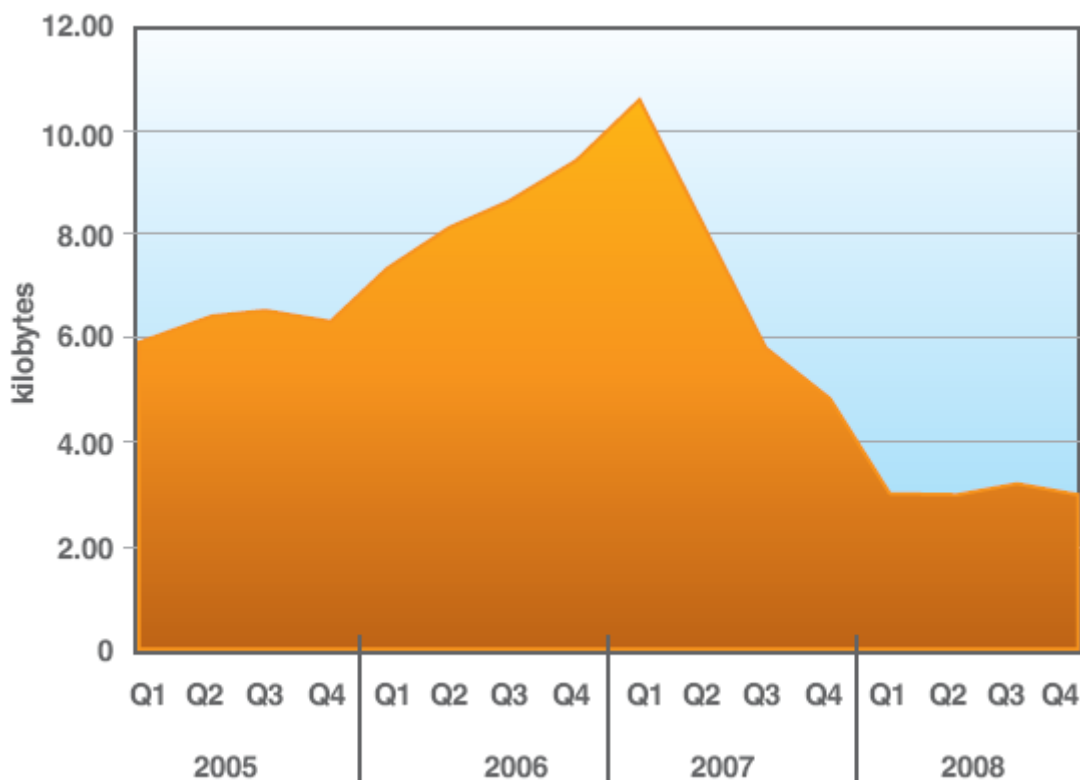


Figura 42: Tamanho Médio de Bytes de Spam Desde 2005

Spam – Linhas de Assunto Mais Populares

Como as linhas de assunto do phishing, as linhas de assunto de spam estão se tornando cada vez mais granulares. As dez principais linhas de assunto de 2008 tomaram conta de uma porcentagem menor de todo o volume de spam em comparação com 2007. À medida que as compras na Internet se tornam cada vez mais populares, os spammers usam assuntos sobre o status de um pedido para atrair o interesse do usuário. Além disso, a oferta de réplicas de relógios e DVDs pornográficos gratuitos parece ser um capturador popular de atenção. A maior parte das outras dez linhas de assunto mais populares não são especialmente indicativas de qualquer tendência particular, à exceção dos "Alertas da CNN", que correspondem à tendência de usar novas URLs em spam, descritas em "Domínios Comuns em Spam de URL", na página 58.

Relatório de Tendências e Riscos da X-Force® 2008

Página 71

A tabela a seguir mostra as linhas de assunto mais populares de spam em 2007 e 2008:

Linhas de Assunto de 2007	%	Linhas de Assunto de 2008	%
Re:	7,18%	Seu pedido	0,43%
<linha de assunto vazia>	2,78%	Re: Status do pedido	0,41%
The Pharmacy America Trusts	2,12%	RE: Mensagem	0,41%
The United States National Associação Médica	1,47%	Réplica de Relógios	0,41%
Fw:	1,47%	Re:	0,38%
Réplica de Relógios	1,12%	Download grátis de DVDs pornográficos	0,23%
Man lebt nur einmal-probiers aus!	0,97%	DVDs pornográficos com download gratuito	0,23%
Pode me dizer o que está errado e como corrigir isto?	0,96%	Réplica Perfeita	o
Você recebeu um cartão eletrônico de um companheiro!	0,85%	Alertas CNN: Meu Alerta Customizado	0,18%
Você recebeu um cartão eletrônico de cumprimentos de um admirador!	0,81%	Olá	0,16%

Tabela 16: Linhas de Assunto Mais Populares de Spam

A Remoção da McColo e Seu Impacto sobre o Spam

Após a retirada do hoster da Web baseado na Califórnia McColo, notamos algumas mudanças significativas em nossa atividade de spam. Do ponto de vista do spam, todo mundo observou uma queda geral. Após a retirada do dia 11 de novembro, o volume de spam em nossas armadilhas de spam caíram cerca de 25% em relação aos níveis anteriores. Mais interessante, talvez, seja a mudança no mercado que observamos nas origens do spam (a localização do país do bot de spam, em geral). Embora o McColo fosse operado fora dos Estados Unidos, as repentinas e extremas mudanças de distribuição por volume e país observadas após o ponto de fechamento apontam o McColo como operador básico de bots de spam no mundo inteiro.

Mudanças na Distribuição Internacional de Spam

Os Estados Unidos têm mantido, durante anos, uma posição superior na lista de origens de spam (veja acima). Seis dias antes da retirada, estava na primeira posição:

5 Principais Países Antes		5 Principais Países Depois		5 Principais Países no Final de 2008	
EUA	14,2%	China	12,7%	Brasil	11,7%
Rússia	11,0%	Rússia	11,4%	EUA	8,1%
Turquia	7,4%	EUA	8,0%	China	6,6%
Espanha	5,9%	Coréia do Sul	6,2%	Turquia	5,7%
Brasil	4,8%	Brasil	5,8%	Rússia	5,7%

Tabela 17: Principais Spammers Antes e Depois da Remoção da McColo

Seis dias após a retirada, a produção de spam advinda dos EUA foi reduzida a meros 14% de sua capacidade original. Portanto, não foi uma terrível surpresa quando os EUA, finalmente, perderam a posição superior da lista no sexto dia após a retirada.

Examinamos mais profundamente o impacto do spam em todo o globo, e a remoção da McColo teve um impacto significativo nos países que talvez não fosse esperada. Por exemplo, toda a produção de spam advinda da Espanha, Índia, Itália, Israel e Turquia foi reduzida a menos de 17% de sua capacidade original de produção. Outros países também foram afetados, embora em menor extensão, conforme indicado no gráfico abaixo:

% da produção anterior de spam

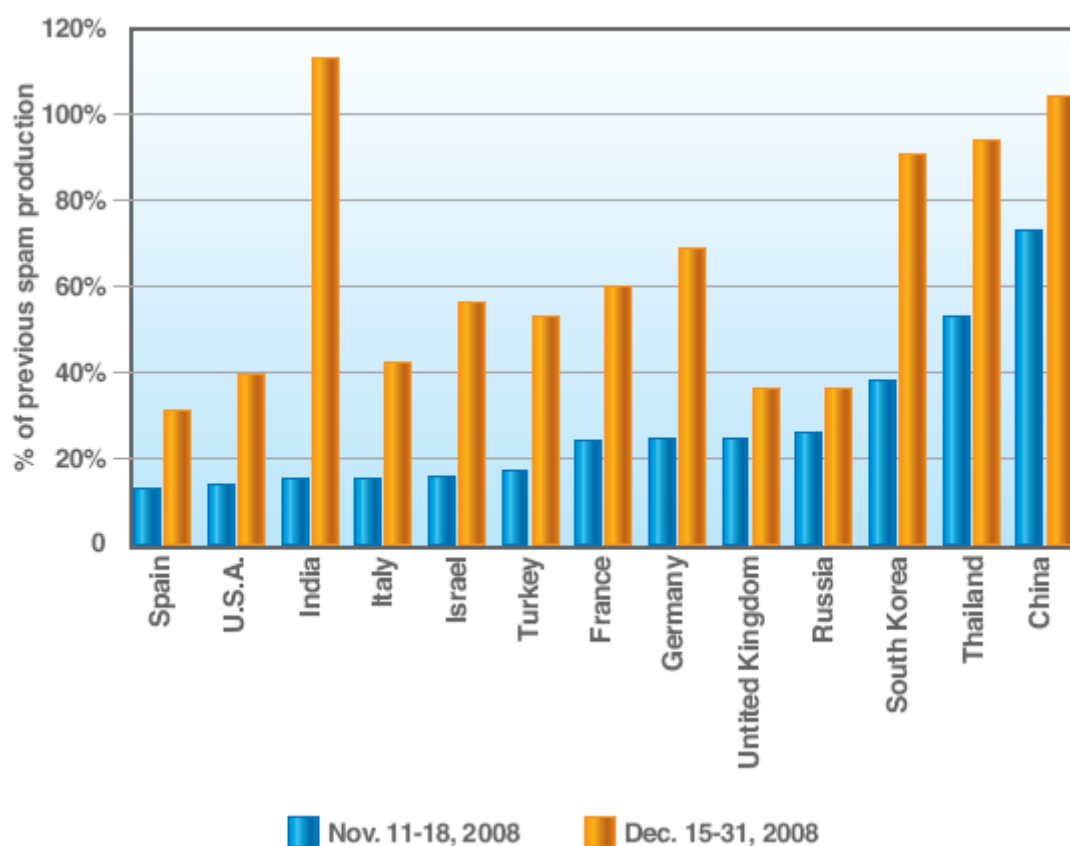


Figura 43: Redução de Spam por País Após o Fechamento da McColo – Nov. 11 – 18, 2008

A segunda barra da Figura 43 indica os países que tiveram a recuperação mais rápida a partir das perdas. Enquanto a Índia e a China recuperaram completamente seus prejuízos, e a Tailândia e a Coreia do Sul chegaram perto da recuperação, muitos outros países ainda produzem bem menos spam do que antes do fechamento.

Mudanças no Conteúdo de Spam

Outras mudanças refletiram-se no volume geral, além do tipo de spam enviado. Os spammers foram forçados a encontrar novas formas de compensar seus prejuízos. Nos primeiros dias, muito pouco mudou. O volume de spam estava simplesmente em baixa. As mudanças nos tipos de spam começaram a aparecer alguns dias depois, conforme demonstra a figura a seguir.

Fechamento da McColo

Percentage Plain-Text Spam	Porcentagem de Spam de Texto Simples
Percentage Image-based Spam	Porcentagem de Spam baseada em Imagem
Percentage URL Spam	Porcentagem de Spam de URL
Week	Semana

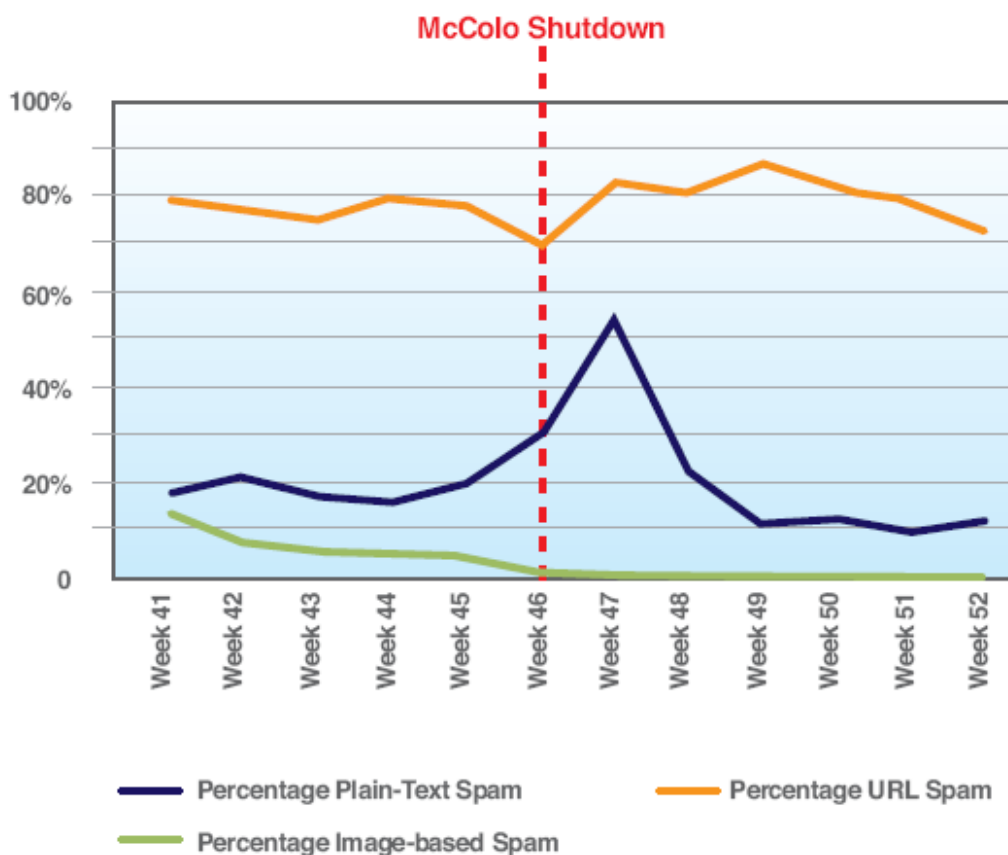


Figura 44: Mudanças no Tipo de Spam após a Remoção da McColo

Após o fechamento, os spammers mudaram para spams de texto simples, simples (sem HTML ou anexos) dentro de alguns dias, o que reverteu a tendência na época, conforme foi visto na Figura 44. Além disto, eles apostaram com maior vigor no spam de URL (antes do fechamento a porcentagem de spam de URL estava abaixo de 80% e após o fechamento estava acima de 80%). Os spammers também deixaram de enviar spam baseado em imagem. É possível que a troca para spam de texto simples tivesse dado aos spammers o caminho mais rápido para livrar-se do novo spam sob estas circunstâncias significativamente diferentes. O custo da criação de imagens extravagantes e layouts de HTML pode ter sido demasiado alto para organizar e distribuir.

Outra razão teria sido que os spammers queriam usar recursos limitados para enviar o maior número possível de spams. Assim sendo, eles apostaram num spam menor (texto simples ou URL) por questões de largura de banda. Estas tendências também são evidentes na análise do tamanho médio de bytes de spam durante esta estrutura:

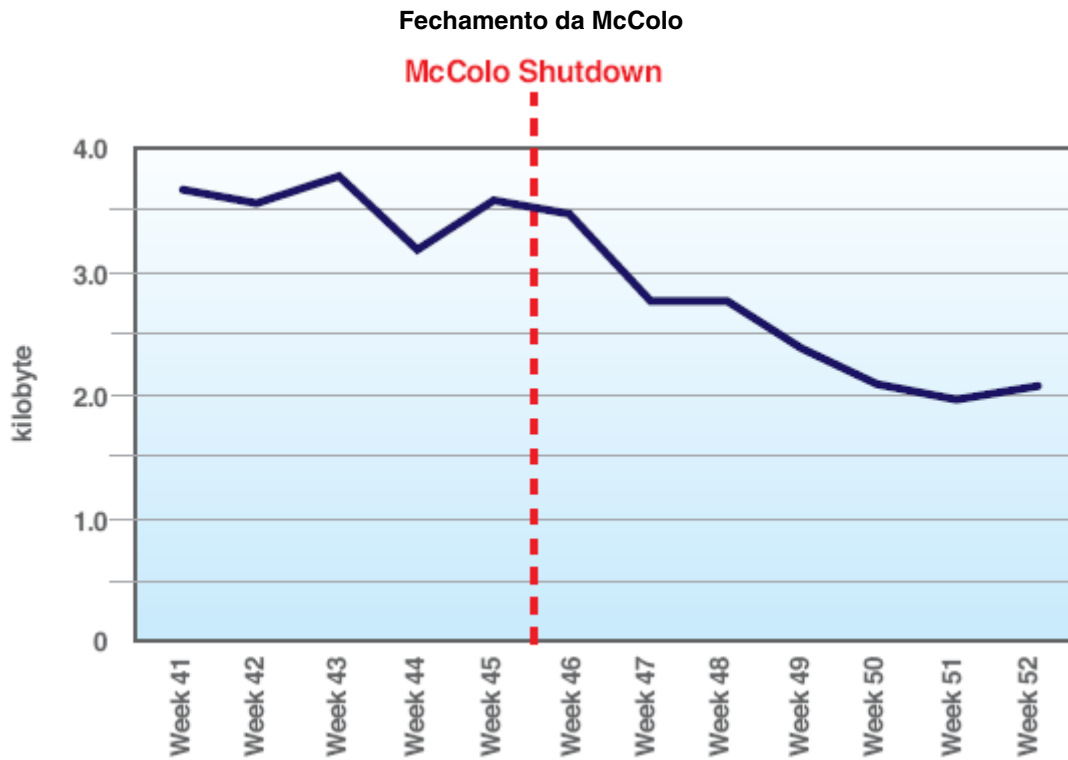


Figura 45: Tamanho Médio de Bytes de Spam Antes e Depois do Fechamento da McColo

Apenas duas semanas após o fechamento da McColo, o volume de spam começou a aumentar. Se a tendência continuar (e pelas antigas taxas de crescimento do volume de spam, vão continuar), o nível anterior de volume de spam provavelmente será alcançado logo no primeiro trimestre de 2009.

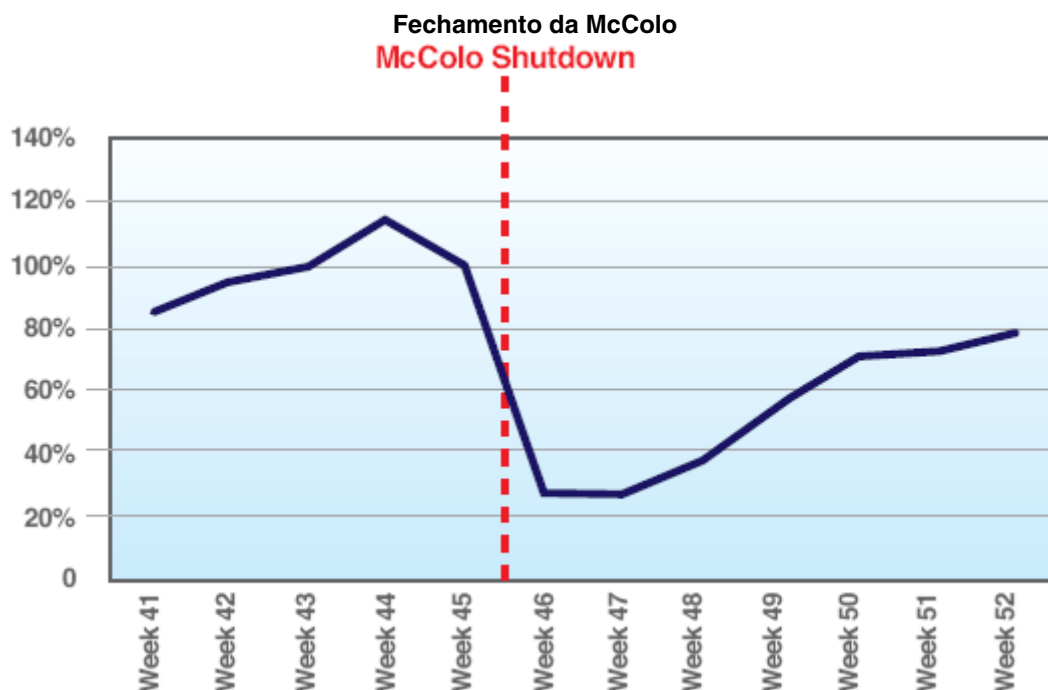


Figura 46: Volume de Spam Antes e Depois da Remoção da McColo

Em resumo, houve duas fases principais após o fechamento da McColo (11 de novembro de 2008):

o Primeira fase (12 de novembro até 23 de novembro): ações de curto prazo empreendidas por spammers, como, por exemplo, aumentar a utilização de spam de texto simples, simples, e parar com o spam baseado em imagem, embora essas mudanças não tenham impactado o volume de spam, que permaneceu baixo durante quase duas semanas.

o Segunda fase (a partir de 24 de novembro, ainda em andamento): redução no tamanho de bytes de spam para largura de banda reserva e aumento no volume de spam. Na época do Natal, a taxa de aumento do volume baixou ligeiramente, mas ainda continua a subir.

Para maiores informações, veja <http://blogs.iss.net/archive/mccolo.html> e <http://blogs.iss.net/archive/mccolo-2.html>.

Phishing

Esta seção aborda os seguintes tópicos:

o Phishing enquanto percentagem de spam

o Tendências do país de origem do phishing, inclusive páginas da Web com phishing (URLs)

o Linhas de assunto mais populares e alvos de phishing

Volume de Phishing

Durante todo o ano de 2008, o volume de phishing era, em média, de 0,5% do volume geral de spam. A percentagem de spam que é phishing está entre 0,4% e 1% com uma queda para 0,2% no segundo trimestre de 2008, e um aumento de 0,8% no segundo período de 2008. Obviamente, os Phishers usaram a crise financeira e a incerteza dos clientes bancários para enviar phishing direcionado este ano. O declínio no último trimestre está mais atrelado ao fechamento da McColo.

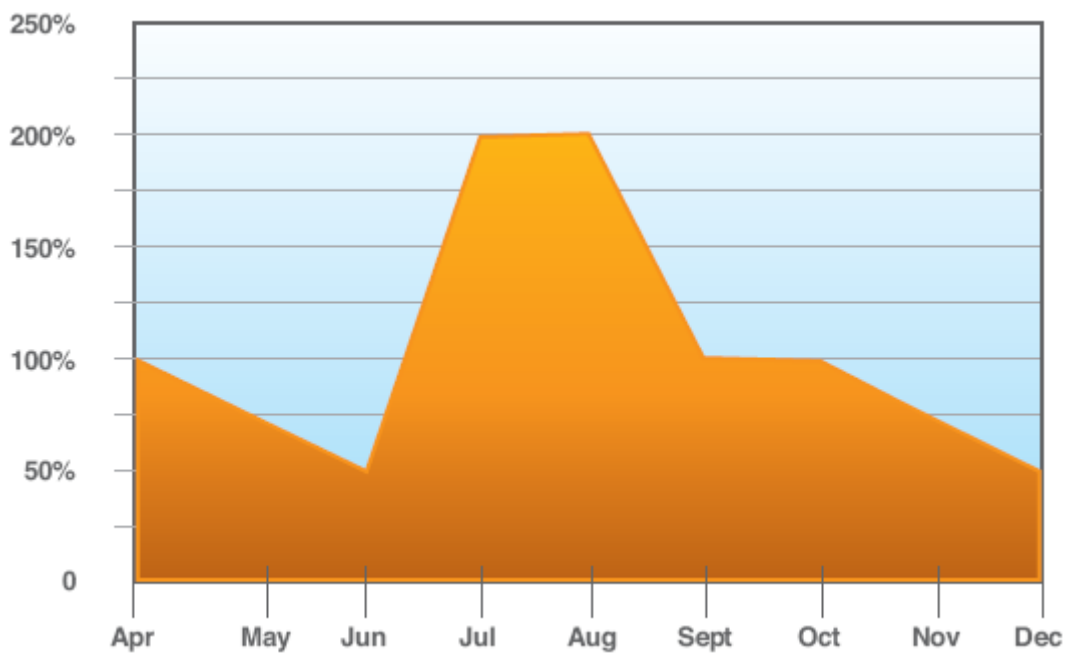


Figura 47: Mudanças no Volume de Phishing em 2008

Phishing – País de Origem

O mapa a seguir destaca os principais países de origem de e-mails com phishing em 2008.

Espanha	15.1%	Israel	6.3%
Itália	14.0%	Polônia	5.5%
Coréia do Sul	10.8%	Alemanha	4.4%
Brasil	7.2%	Argentina	3.0%
França	6.4%	E.U.A.	2.8%

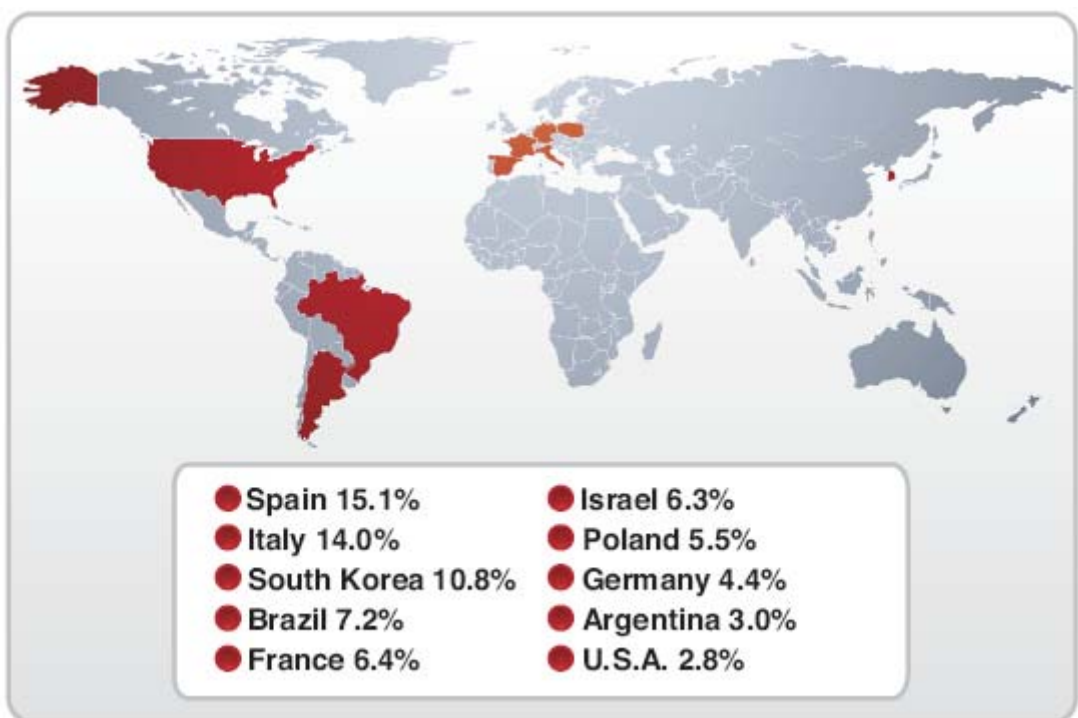


Figura 48: Distribuição Geográfica de Emissores de Phishing

Phishing – Tendências do País de Origem

Nos últimos três anos, a Itália e a Coréia surgiram como principais emissores de phishing, enquanto a Espanha permanece como a origem principal incontestada dos e-mails com phishing. Israel e Brasil, embora apresentando ligeira queda em 2008, ainda são as maiores fontes de e-mails com phishing.

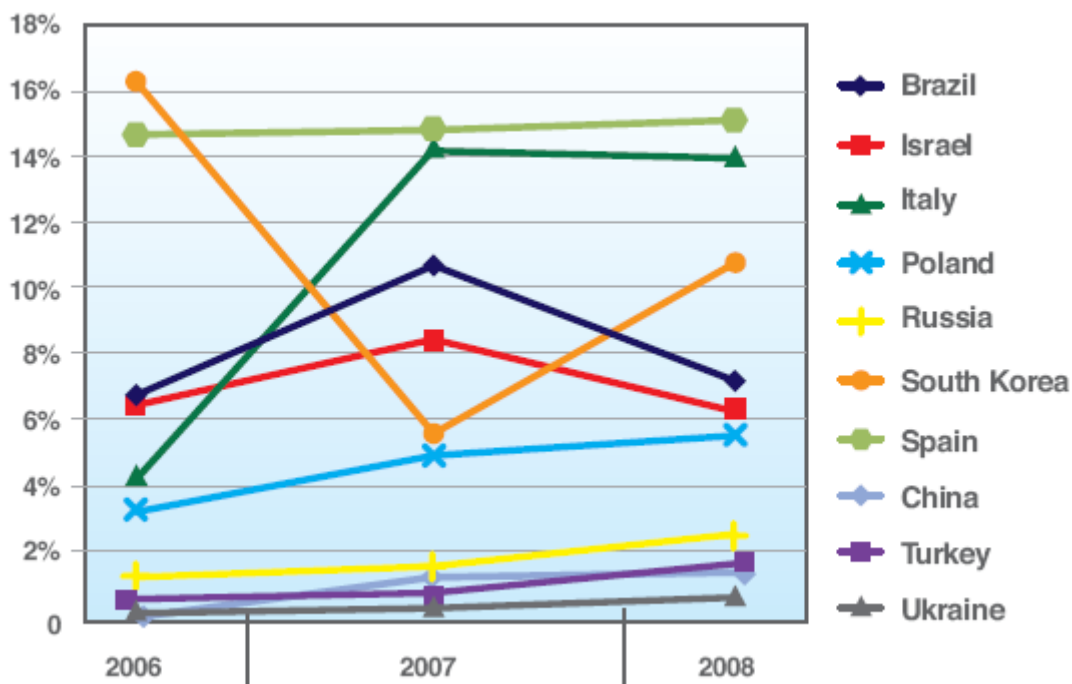


Figura 49: Tendências de Origem de Phishing: Beneficiários e Sustentadores a Longo Prazo

Diversos países mostraram quedas significativas como fontes de phishing, principalmente Estados Unidos e França.

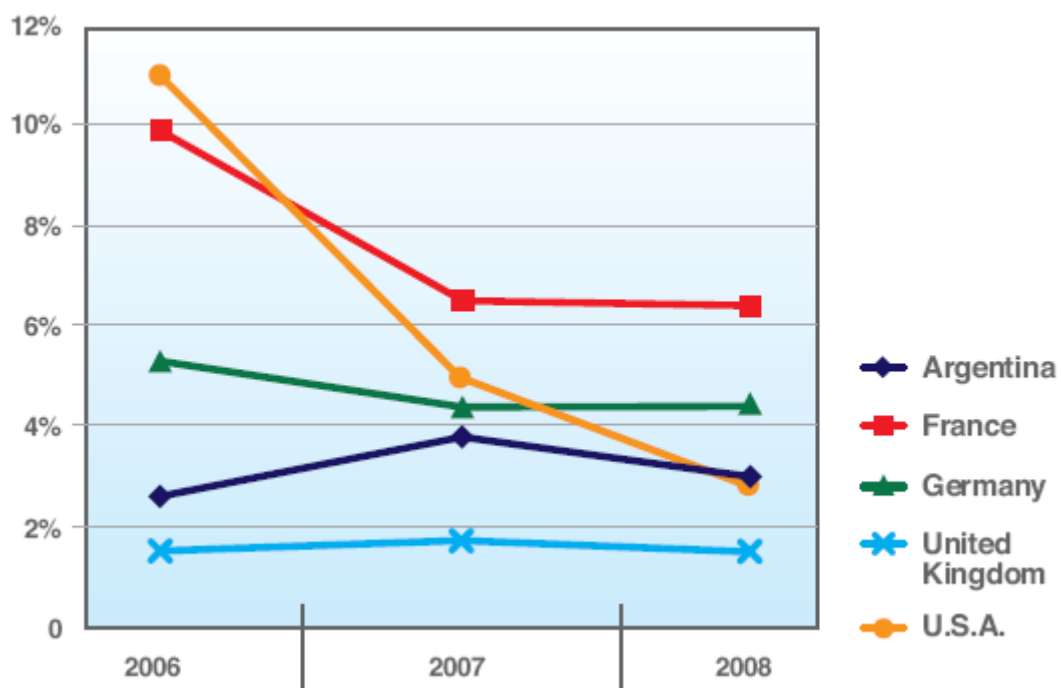


Figura 50: Tendências de Origem de Phishing: Declinantes a Longo Prazo

URLs com Phishing – País de Origem

O mapa a seguir mostra onde estão hospedadas as URLs com Phishing.

E.U.A.	20,2%	Rússia	5,4%
Cingapura	18,9%	Reino Unido	2,6%
Coréia do Sul	17,1	Japão	2,3%
Romênia	8,8%	China	2,2%
Canadá	5,4%	Tailândia	1,7%

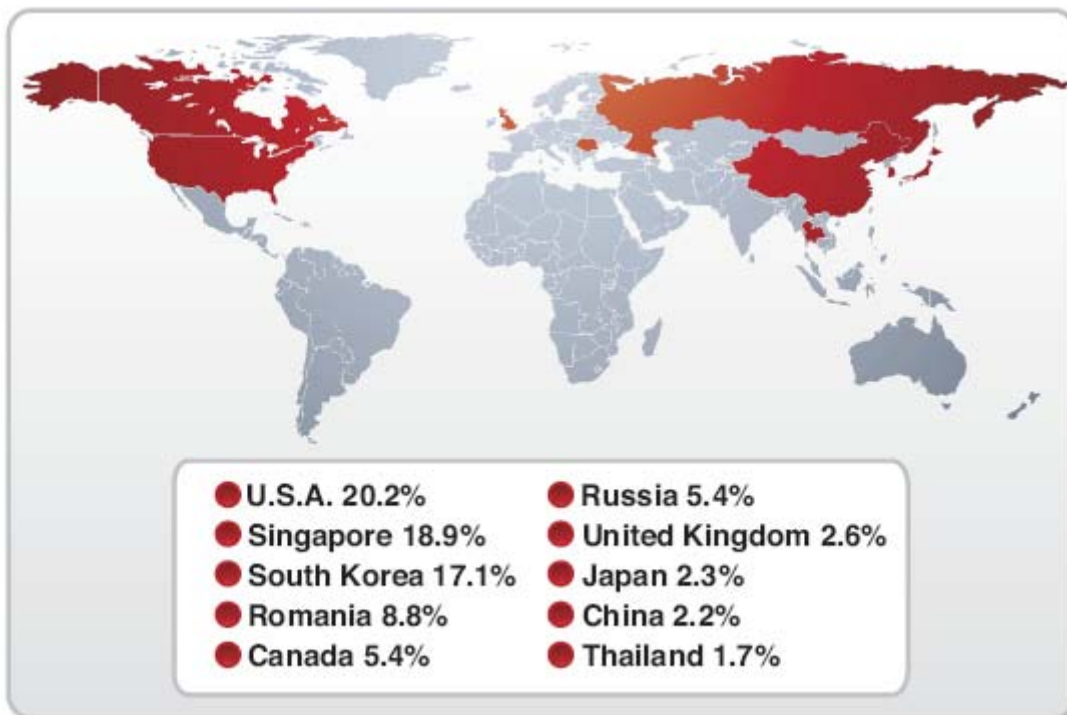


Figura 51: Distribuição Geográfica de URLs com Phishing

URLs com Phishing – Tendências do País de Origem

Nos últimos três anos, ocorreram muitas mudanças nos principais países que hospedam URLs com Phishing: apesar da queda drástica ocorrida nos EUA, o país continua sendo o principal host de URLs com Phishing, porém sabe-se há pouco tempo que Cingapura e a Coreia do Sul não ficam muito atrás:

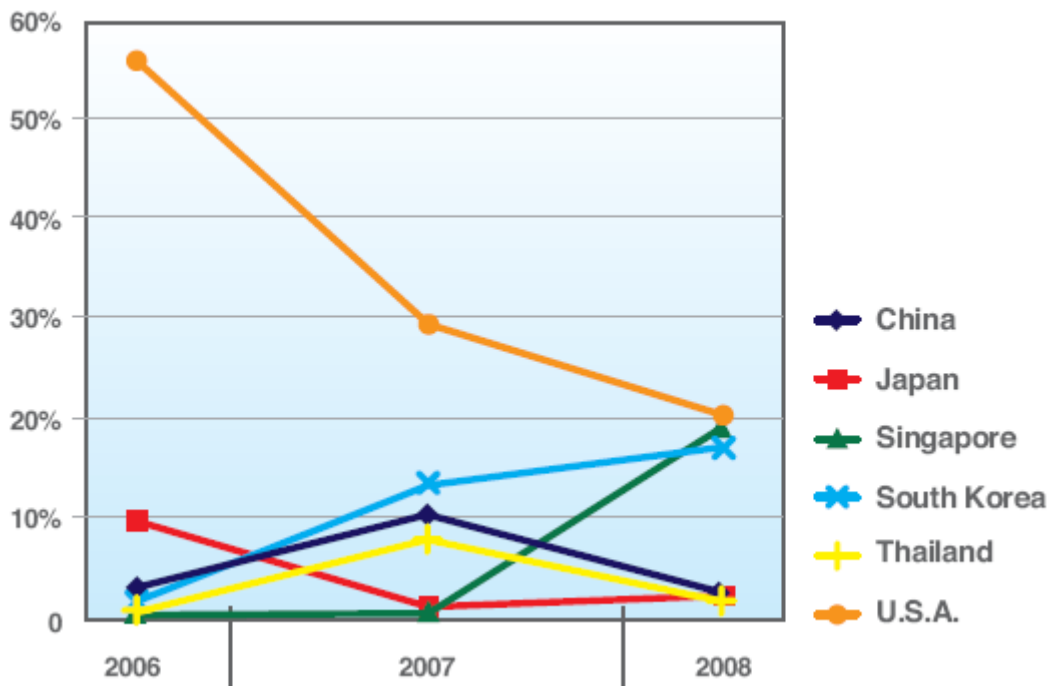


Figura 52: Hosts de URL com Phishing, Principais Contribuintes

Outros países a observar são Romênia, Canadá e Rússia. Estes países mostraram aumentos significativos no ano passado:

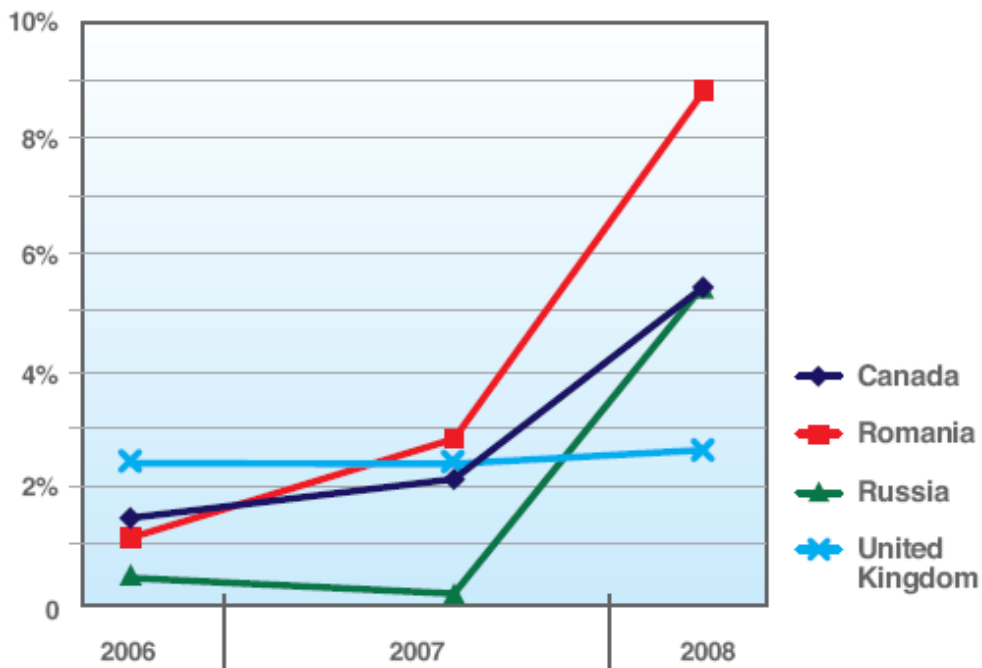


Figura 53: Hosts de URL com Phishing: Beneficiários e Sustentadores a Longo Prazo

Diversos países apresentaram quedas significativas no número de hosts de URL com Phishing – principalmente Cazaquistão e Alemanha.

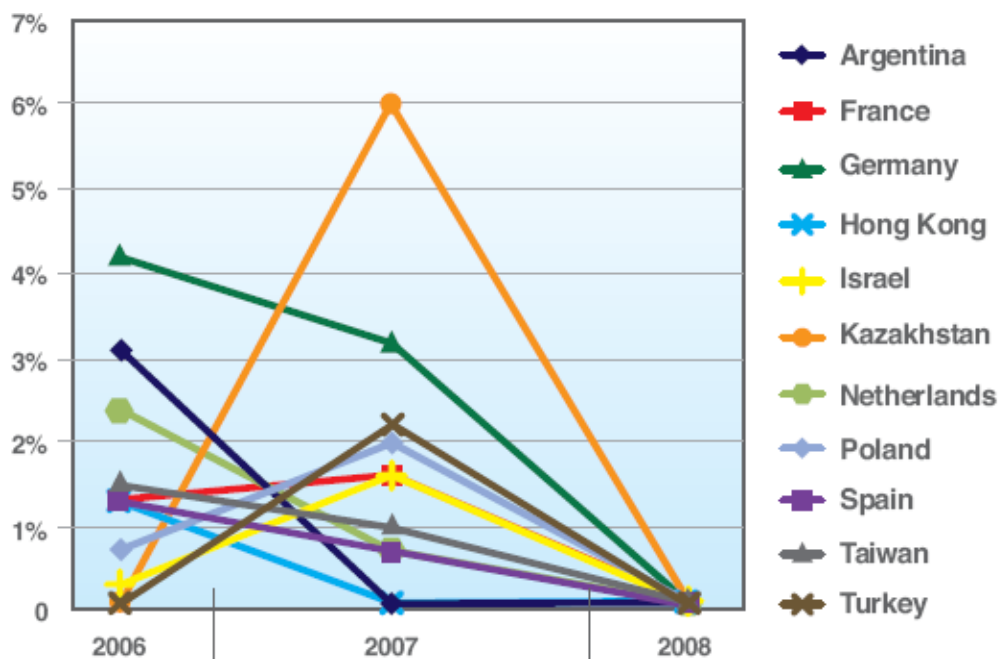


Figura 54: Hosts de URL com Phishing: Declinantes a Longo Prazo

Phishing – Linhas de Assunto Mais Populares

Uma das maiores mudanças em 2008 é que as linhas de assunto populares já não são tão populares. Em 2007, as linhas de assunto mais populares representavam cerca de 40% de todos os e-mails com phishing. Em 2008, as linhas de assunto mais populares reuniram apenas 6,23% de todas as linhas de assunto de phishing. A implicação é que os phishers estão se tornando mais granulares em seus alvos, essencialmente com a maior variação nas linhas de assunto de todos os tempos. Outra tendência que se desenvolveu em 2008 é o foco na ação do usuário. Em vez de ter um assunto genérico, tipo "alerta de segurança", os phishers tentam comprometer o usuário com alguma ação, tipo recuperar uma conta que foi suspensa ou atualizar os dados de sua conta. A tabela a seguir mostra as linhas de assunto mais populares de phishing em 2007 e 2008:

Linhas de Assunto de 2007	%	Linhas de Assunto de 2008	%
<linha de assunto vazia>	22,21%	Departamento de Análise de Conta PayPal®	1,47
Medidas de Segurança da Conta!	3,86%	Departamento de Segurança do PayPal	0,97
Aviso Importante – E*TRADE FINANCIAL Corp	3,21%	Departamento de Mau Uso do PayPal	0,63
Aviso Importante!	2,01%	Medidas de Segurança de Conta PayPal	0,60
Volksbanken Raiffeisenbanken AG: 02/11/2007	1,94%	Volksbanken Raiffeisenbanken	0,48
Medidas de Segurança!	1,82%	Suspensão de Conta PayPal	0,47
Segurança de Conta do Citibank !	1,77%	Recupere sua Conta no Barclays	0,44
Aviso do Citibank!	1,75%	Leia com atenção – Notificação Importante	0,40
Medidas de Segurança de Conta do Citibank!	1,74%	Atualize os Dados da sua Conta.	0,30
Volksbanken Raiffeisenbanken AG: 14/11/2007	1,32%	Leia com atenção – Notificação Importante!	0,38

Tabela 18: Linhas de Assunto Mais Populares de Phishing

Alvos de Phishing

Phishing – Alvos por Indústria

Em 2008, a maior parte do phishing – aproximadamente 90% – objetivava instituições financeiras. Sete por cento dos alvos eram serviços de pagamento on-line e menos de 5% miravam outras indústrias (como Web sites de leilões on-line, serviços de comunicações e lojas on-line):

Instituições Financeiras	88,2%
Pagamentos On-line	7,2%
Outros	4,6%

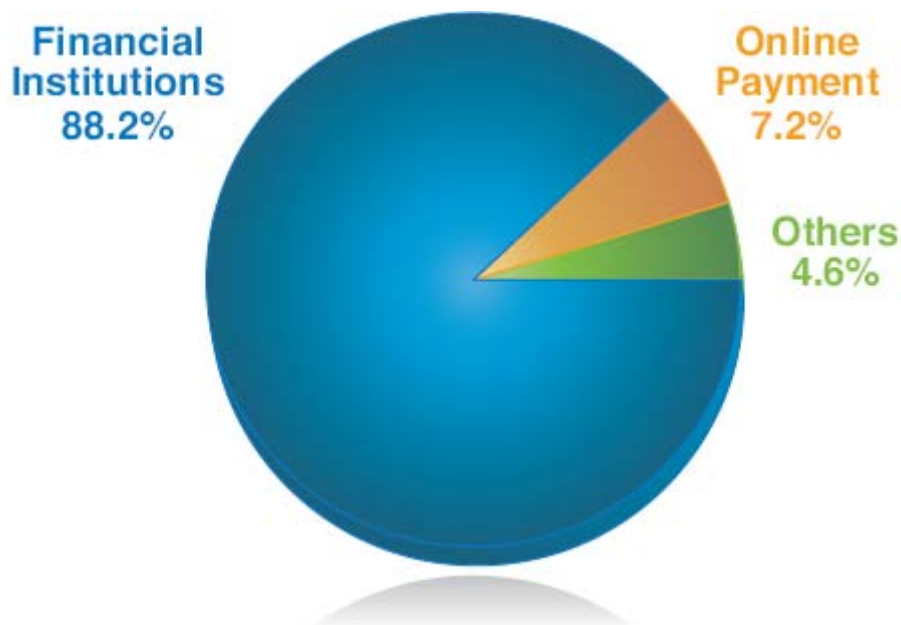


Figura 55: Phishing por Indústria, 2008

Phishing – Alvos Financeiros por Geografia

Mais de 99% dos alvos de phishing financeiros estão na América do Norte ou na Europa, a maioria na América do Norte (58,4%).

América do Norte	58,4%
Europa	40,8%
Outros	0,8%

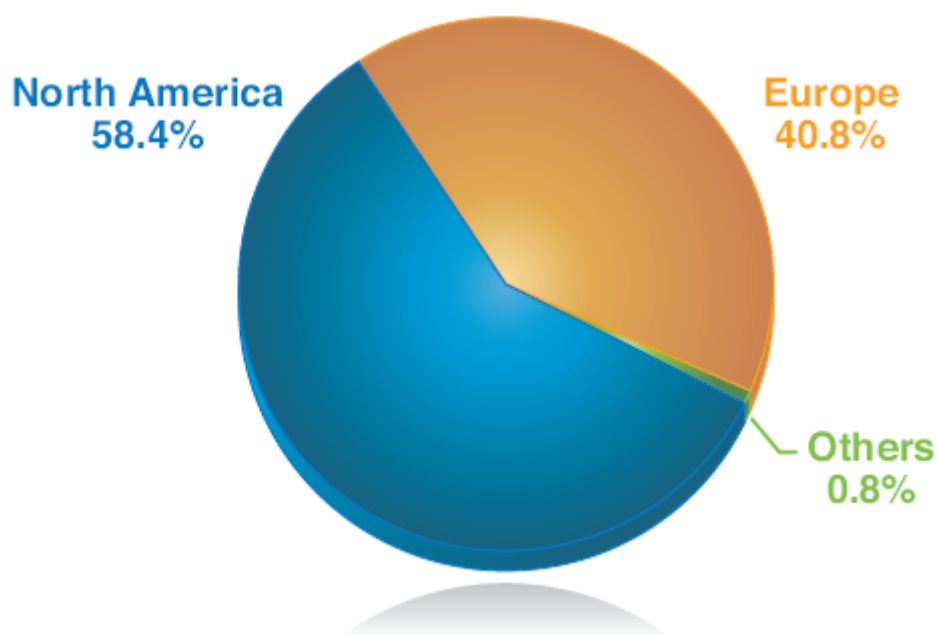


Figura 56: Phishing Financeiro por Localização Geográfica, 2008

Tendências de Conteúdos da Web

Esta seção resume a quantidade e a distribuição de conteúdo "ruim" na Web, normalmente indesejado pelas empresas com base nos princípios sociais e na política corporativa. O conteúdo indesejado ou "ruim" da Internet está associado com três tipos de Web sites: adultos, desvio de comportamento social e criminoso. A Tabela 19 lista as categorias de filtros da Web IBM ISS que correspondem a estes tipos de sites.

As categorias de filtro da Web são definidas com detalhes em:

<http://www.ibm.com/services/us/index.wss/detail/iss/a1029077?cntxt=a1027244>

Tipo de Web Site	Descrição e Categoria de Filtro da Web
Adultos	Pornografia Erótico / Sexo
Desvio de Comportamento Social	Política Excessiva / Ódio / Discriminação Seitas
Criminoso	Proxies Anônimos Crime por Computador / Hacking Atividades Ilícitas Drogas Ilícitas Malware Violência / Excessos Warez / Pirataria de Software

Tabela 19: Categorias de Filtros da Web Associados com Conteúdo Indesejado na Web

Esta seção apresenta a análise de:

- o Percentual e distribuição de conteúdo na Web considerado ruim, indesejado ou indesejável*
- o Percentual e distribuição de conteúdo adulto*
- o Percentual e distribuição de conteúdo com desvio de comportamento social*
- o Percentual e distribuição de conteúdo criminoso*
- o Aumento na quantidade de proxies anônimos*

Metodologia da Análise

A X-Force capturou informações sobre a distribuição de conteúdos na Internet pela contagem de hosts categorizados no banco de dados de filtros IBM ISS. A contagem de hosts é um método aceito para determinar a distribuição de conteúdos e oferece a avaliação mais realista de todas. Quando se usa outras metodologias – como a contagem de páginas/subpáginas da Web – os resultados podem ser diferentes.

O centro de dados IBM ISS está constantemente revisando e analisando novos conteúdos de dados da Web. Examine a estatística a seguir, relacionada com o centro de dados IBM ISS:

- o Analisa 150 milhões de novas páginas e imagens na Web por mês*
- o Analisou 9,1 bilhões de páginas e imagens na Web desde 1999*

O IBM ISS Web Filter Database contém:

- o 68 categorias de filtros*
- o 100 milhões de entradas*
- o 150.000 entradas novas ou atualizadas acrescentadas por dia*

Percentual de Conteúdo Indesejado na Internet

Atualmente, há cerca de 8% de conteúdo indesejado na Internet, como, por exemplo Web sites pornográficos ou criminosos.

Outros	Adulto	Criminoso	Desvio de Comportamento Social
91,945%	7,826%	0,226%	0,003%

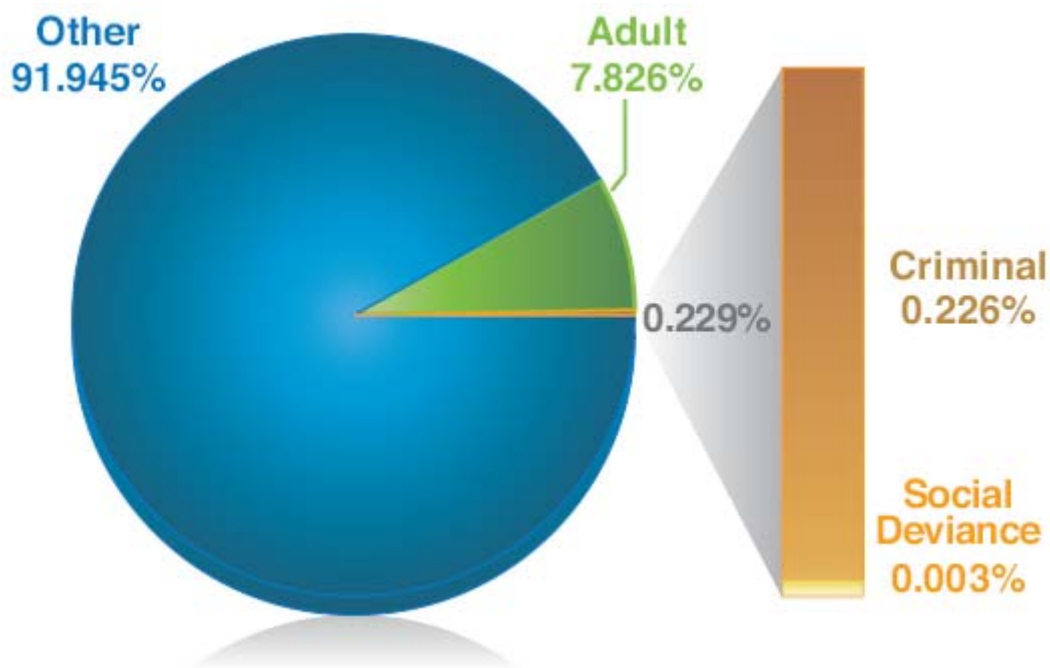


Figura 57: Distribuição de Conteúdos da Internet, 2008

Relatório de Tendências e Riscos da X-Force® 2008

Página 89

Distribuição Geográfica de Conteúdo Adulto

E.U.A.	52,1%	Canadá	4,2%
Alemanha	15,7%	França	3,5%
Países Baixos	5,1%	Reino Unido	1,4%
Rússia	4,7%	China	1,2%
Coréia do Sul	4,4%	Polônia	0,8%

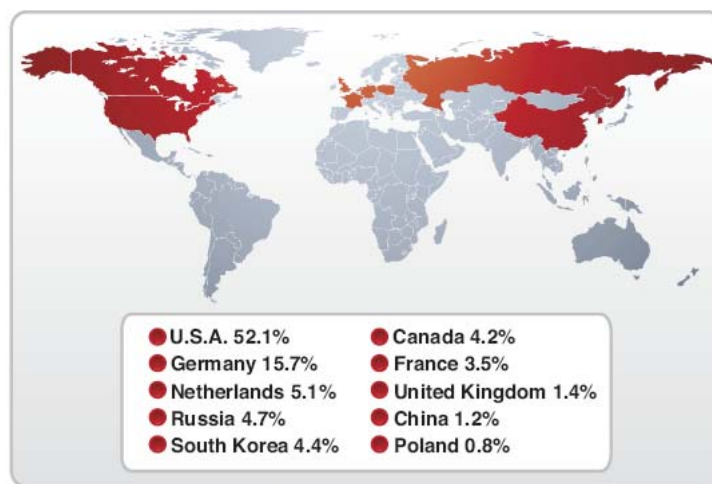


Figura 58: Distribuição Geográfica de Conteúdo Adulto

Distribuição Geográfica de conteúdo com Desvio Social

E.U.A.	50,6%	França	2,5%
Alemanha	17,8%	Reino Unido	2,0%
Países Baixos	7,4%	Itália	1,3%
Canadá	7,2%	Rússia	0,7%
China	4,8%	Japão	0,5%

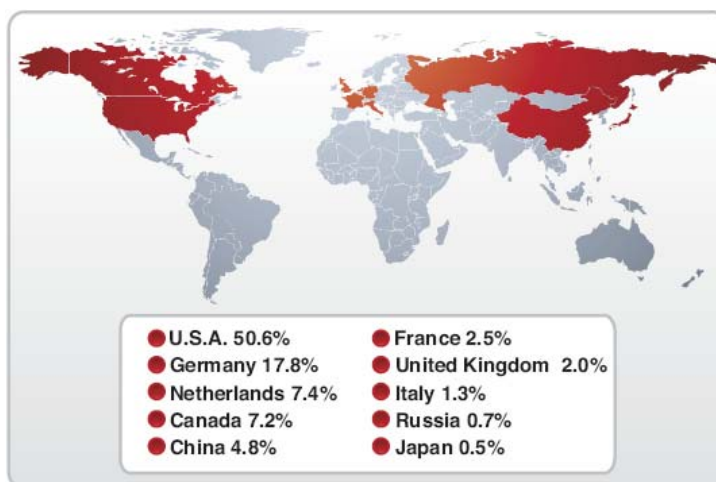
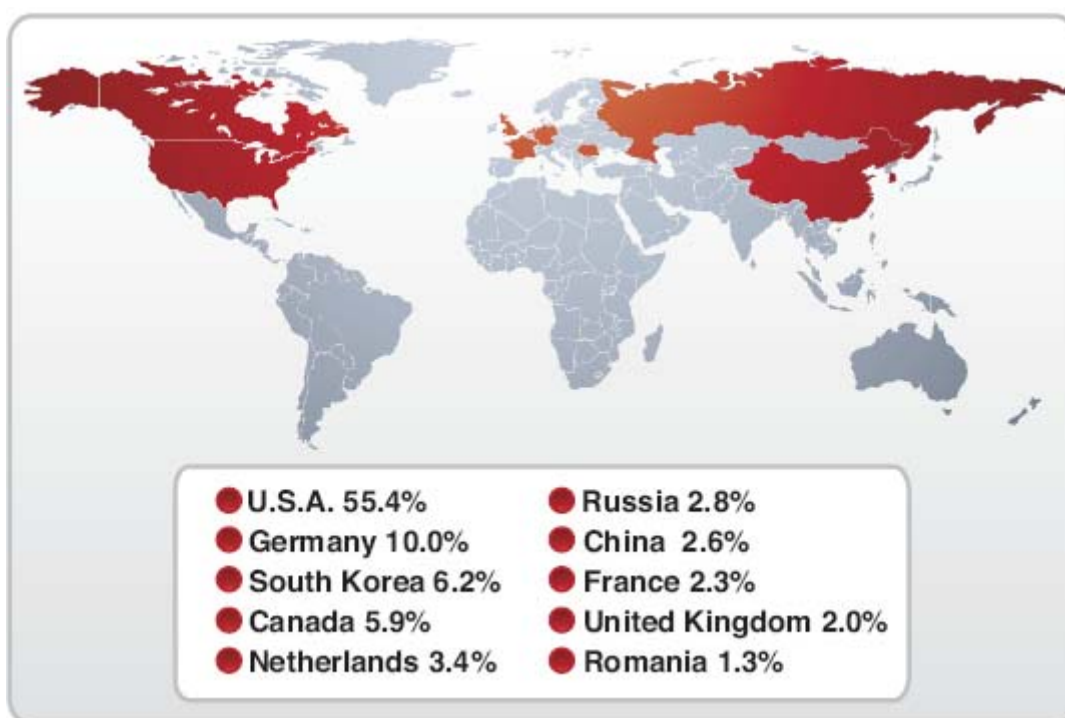


Figura 59: Distribuição Geográfica de Conteúdo com Desvio de Comportamento Social

Distribuição Geográfica de Conteúdo Criminoso

E.U.A.	55,4%	Rússia	2,8%
Alemanha	10,0%	China	2,6%
Coréia do Sul	6,2%	França	2,3%
Canadá	5,9%	Reino Unido	2,0%
Países Baixos	3,4%	Romênia	1,3%

*Figura 60: Distribuição Geográfica de Conteúdo Criminoso*

Aumento de Proxies Anônimos

À medida que a Internet faz parte cada vez mais de nossas vidas, não apenas em casa, como também no trabalho e na escola, as organizações responsáveis pela manutenção de ambientes aceitáveis estão sempre descobrindo a necessidade de inserir controles nos locais onde as pessoas podem navegar nestas configurações públicas. Um desses controles é um sistema de filtragem de conteúdos, que evita o acesso a Web sites inaceitáveis ou impróprios, conforme está descrito nesta seção do Relatório de Tendências. Num esforço para dar a volta nas tecnologias de filtragem da Web, algumas pessoas devem tentar usar um Proxy Anônimo (também conhecido como Proxy da Web).

Os proxies da Web permitem que os usuários registrem uma URL num formulário da Web em vez de visitar diretamente o Web site alvo. Usando os proxies, escondem o URL alvo de um filtro da Web. Se o filtro da Web também não estiver configurado para monitorar ou bloquear Proxies Anônimos, esta atividade, que teria normalmente sido interrompida, passará pelo filtro e permitirá que o usuário alcance a página da Web não autorizada. O índice de aumento de Web sites com Proxy Anônimo reflete esta tendência:

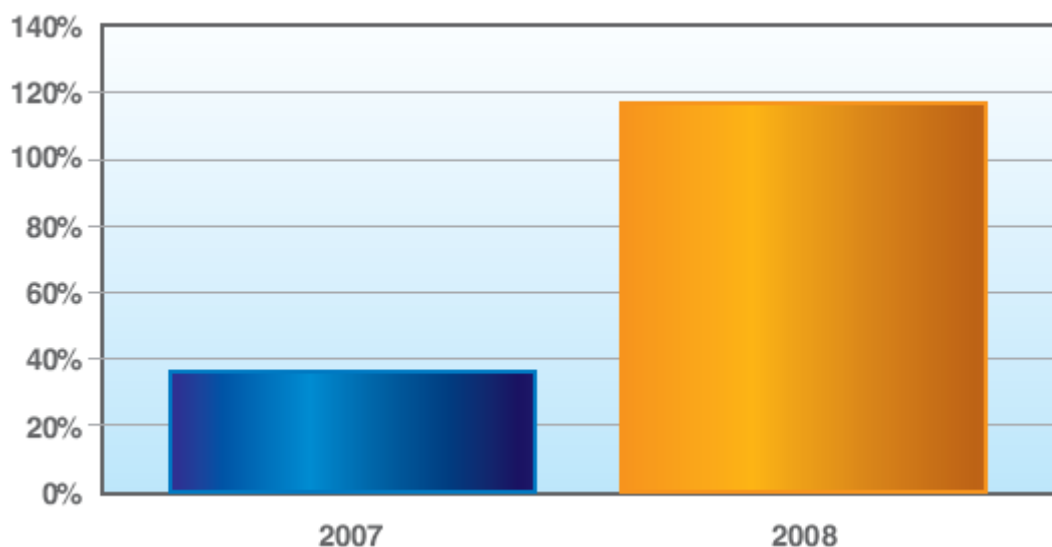


Figura 61: Aumento Ano após Ano da Incidência de Proxies Anônimos em Web Sites

Em 2007, o número de proxies anônimos aumentou em cerca de 1/3. Em 2008, o número mais do que dobrou em comparação com o ano de 2007.

Tendências de Malware

Tendências da Categoria de Malware

O gráfico a seguir mostra a percentagem de malware de cada uma das principais categorias em 2008:

Cavalo de Tróia	46%
Outros	17%
Worm	14%
Backdoor (porta dos fundos)	12%
PUP (Programas Potencialmente Indesejáveis)	6%
Vírus	5%

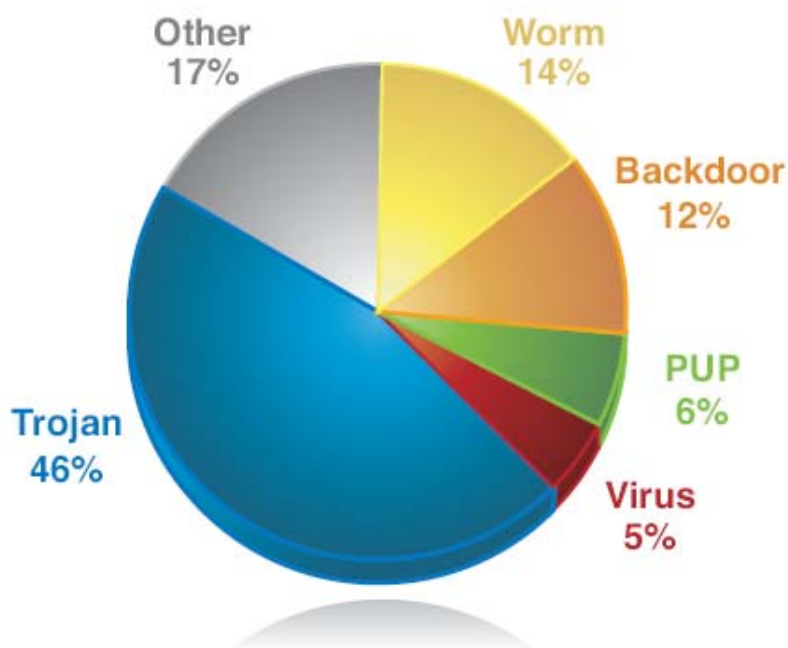


Figura 62: Malware por Categoria, 2008

As principais categorias de malware são:

o **Vírus** – se propaga infectando um arquivo host.

o **Worm** – se auto-propaga através de e-mail, redes compartilhadas, unidades removíveis, compartilhamento de arquivos ou aplicativos de mensagens instantâneas.

o **Backdoor** – oferece funcionalidade para que um atacante remoto se registre e/ou execute comandos arbitrários no sistema afetado.

o **Cavalo de Tróia** – desenvolve uma série de funções maliciosas como espionagem, roubo de informações, teclados de registro (logging keystrokes) e download de malware adicional.

o **Potentially Unwanted Programs (PUP)** – programas que o usuário permite que sejam instalados, e que podem afetar a postura de segurança do sistema ou serem usados para finalidades maliciosas. Exemplos: Adware, Dialers e Hacktools/"ferramentas de hackers" (inclusive analisadores, scanners de porta, "constructor kits" de malware, etc.)

o **Outros** – programas maliciosos não classificados que não se enquadram nas outras categorias principais.

Estrutura da Funcionalidade do Cavalo de Tróia

Como um grande percentual de malware foi classificado como Cavalos de Tróia em 2008, é importante levar em consideração como a funcionalidade deles varia. Os dados abaixo mostram a estrutura e a tendência da categoria Cavalos de Tróia em 2008.

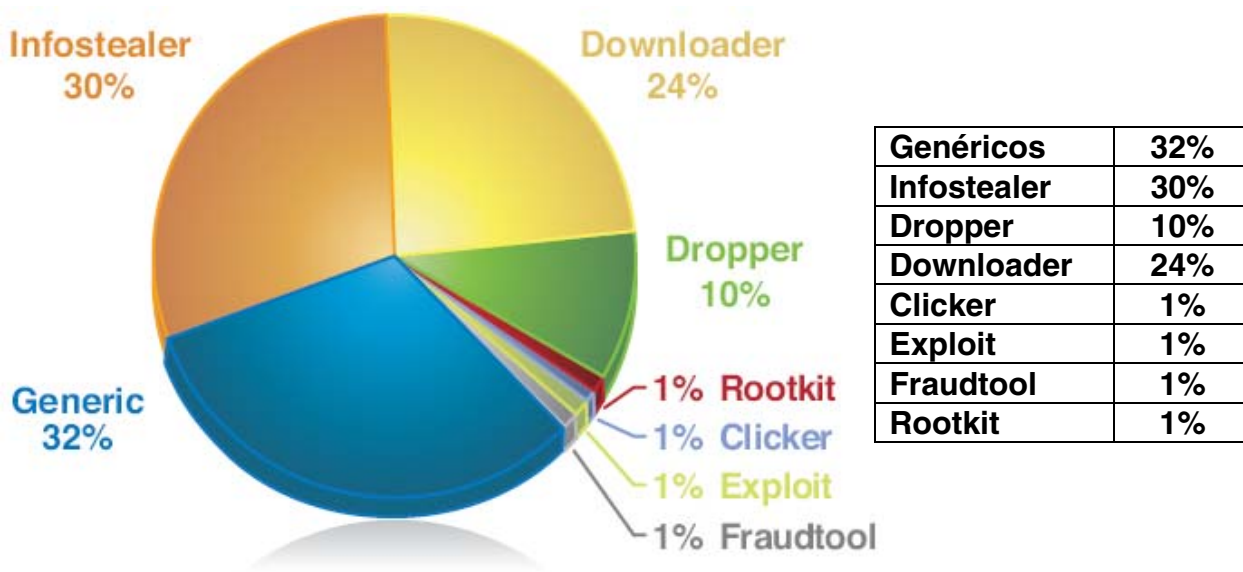


Figura 63: Cavalos de Tróia por Categoria, 2008

As subcategorias do cavalo de tróia são as seguintes:

o **Infostealer** – espões e/ou roubos de informações; entre eles estão ladrões de senhas, registradores de teclado e spyware.

o **Downloader** – faz o download de um ou mais componentes de malware de um site remoto e em seguida os instala no sistema afetado.

o **Dropper** – cai e instala um ou mais componentes de malware num sistema afetado.

o **FraudTool** – malware usado para cometer fraudes, por exemplo, um malware que exibe mensagens falsas de erros ou infectadas e, em seguida, atrai o usuário para comprar ferramentas ou software de segurança falsos.

o **Clicker** – gera tráfego de Web sites cuja finalidade é gerar receita ou outros objetivos maliciosos.

o **Rootkit** – componentes usados por outro malware para ter a capacidade de ocultar-se do usuário e do software de segurança.

o **Exploit** – documentos ou arquivos de mídia contendo código de exploit.

o **Proxy** – permite que um atacante remoto retransmita conexões através do sistema afetado para ocultar sua origem real.

o **Genéricos** – cavalos de tróia que não se enquadram em outras subcategorias.

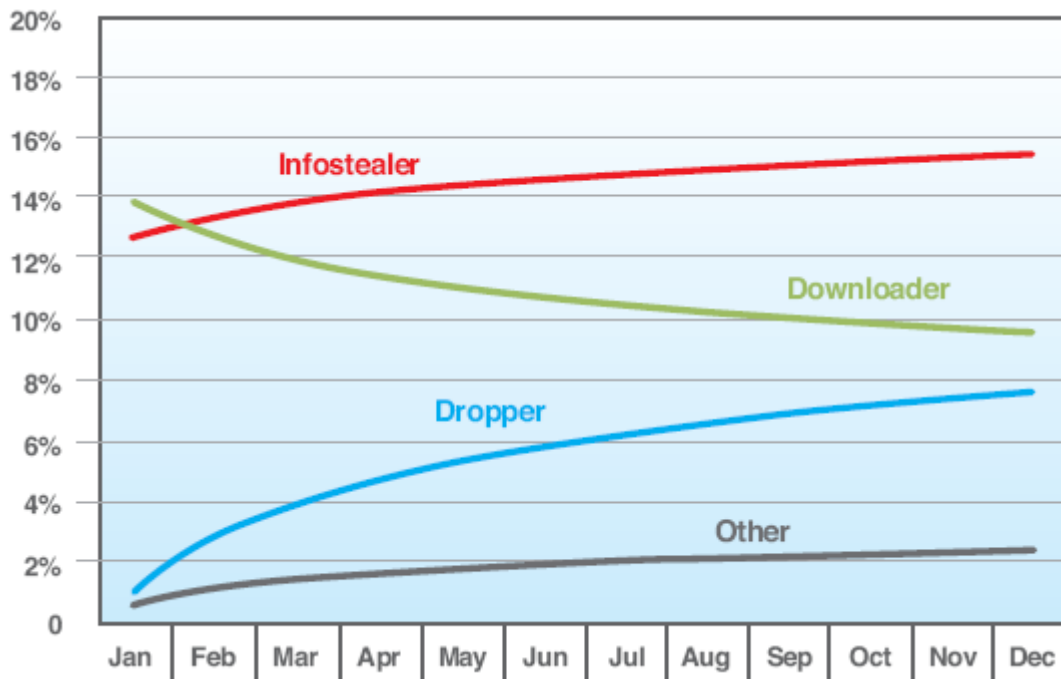


Figura 64: Tendências do Cavalo de Tróia, 2008

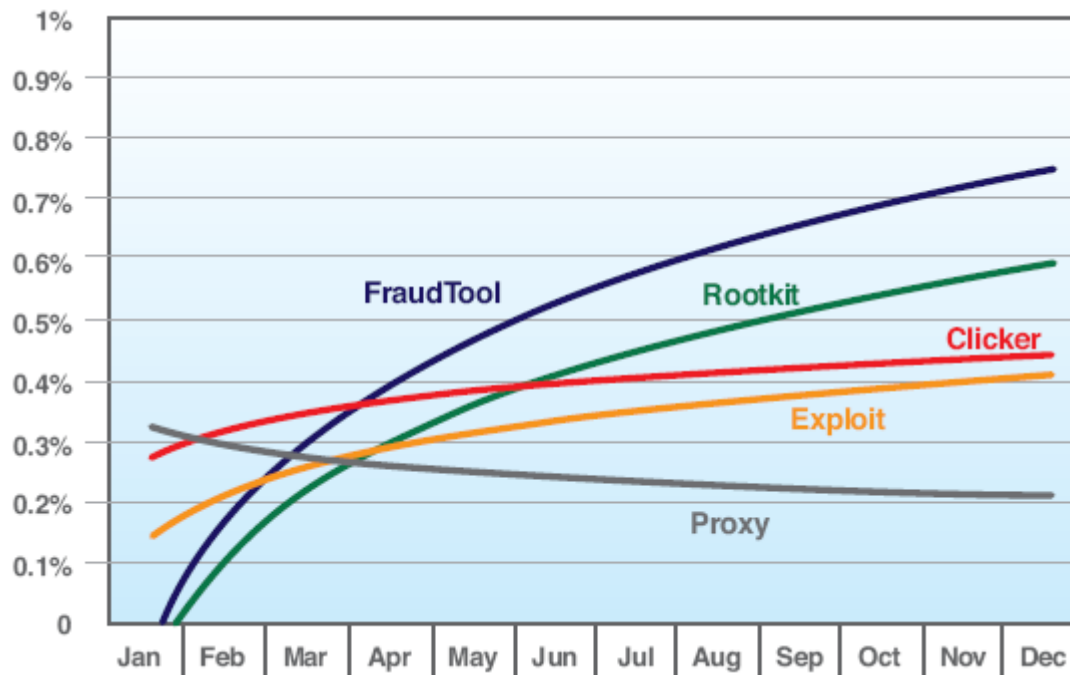


Figura 65: Tendências do Cavalo de Tróia, Detalhe Granular de Outra Categoria, 2008

Análise e Descobertas

o A categoria de malware mais predominante é o cavalo de tróia, que compreende 46% de nossa coleção de malware.

o As subcategorias mais comuns de cavalos de tróia (sem contar a subcategoria Genéricos) são Infostealers (30%), seguida pelos Downloaders (24%) e pelos Droppers (10%). A tendência também mostra que a proporção de Infostealers e Droppers aumentou durante o ano.

o A predominância de cavalos de tróia Infostealer sugere que os atacantes querem sempre espiar e roubar informações dos usuários. Uma grande percentagem destes cavalos de tróia Infostealer são aqueles que miram nos jogos on-line (38% de Infostealers) e usuários de operações bancárias on-line (18% de Infostealers).

o A predominância de Downloaders e Droppers sugere o uso contínuo de estratégia multicomponentes/ multiestágios em que se faz o download ou se deixa cair componentes adicionais de malware depois que o sistema está comprometido.

Famílias de Malware Predominante

A tabela abaixo lista as famílias mais comuns de malware em 2008; famílias genéricas como o Agent ou Delf não estão incluídas na lista:

Posição	Família	Categoria
1	Allaple	Worm
2	Onlinegames	Cavalo-de-Tróia-Infostealer
3	Vírut	Vírus
4	Hupigon	Backdoor (porta dos fundos)
5	Banker	Cavalo-de-Tróia-Infostealer
6	Swizzor	Cavalo-de-Tróia-Downloader
7	Banload	Cavalo-de-Tróia-Downloader
8	Ardamax	Cavalo-de-Tróia-Infostealer
9	Bífroze	Backdoor
10	Rbot	Backdoor
11	Ldpinch	Cavalo-de-Tróia-Infostealer
12	Poison	Backdoor
13	Zlob	Cavalo-de-Tróia-Downloader
14	Kgen	Cavalo-de-Tróia-Dropper
15	Autorun	Worm
16	Ircbot	Backdoor
17	Virtumonde	PUP-Adware
18	Magania	Cavalo-de-Tróia-Infostealer
19	Adultbrowser	PUP-Dialer
20	Bagle	Cavalo-de-Tróia-Downloader

Tabela 20: Famílias de Malware Mais Predominante, 2008

Análise e Descobertas

o Estas 20 maiores famílias de malware predominante compreendem 35% de nossa coleção de malware.

o Allaple, worm de rede que se propaga através de redes compartilhadas e explorando vulnerabilidades, se mantém na posição número 1 em 2008.

o Os cavalos de tróia que objetivam usuários de jogos on-line (Onlinegames, Magania) e operações bancárias on-line (Banker e Banload) continuam predominantes durante o ano inteiro; o que indica que estes grupos específicos de usuários foram altamente visados em 2008.

o Todas as backdoors (Hupigon, Bifrose, Poison, Rbot e Ircbot), incluídas entre as 20 principais, são famílias que disponibilizam um “constructor kit” ou código-fonte.

o Aparte o Allaple, o único outro Worm que conseguiu ser um dos 20 principais é o Autorun, sugerindo que através de unidades/dispositivos removíveis continua a tornar-se um método popular de propagação.

Eventos Notáveis de Malware em 2008

Esta seção discute resumidamente alguns dos eventos notáveis de malware que aconteceram em 2008.

MBR Rootkits

Nas últimas semanas de 2007, um novo malware chamado Mebroot (também conhecido como Mbroot/StealthMBR), que usa uma técnica muito antiga para roubar, foi descoberto primeiro durante a disseminação³ e variáveis adicionais dele foram vistas em 2008. Um recurso interessante do Mebroot é que ele usa uma técnica antiga, empregada por vírus datados, roubados de boot de DOS. Isto é, ele tenta roubar colocando seu código carregador no MBR (Master Boot Record) para que ele obtenha o controle do sistema antes do sistema operacional e depois redireciona o código (neste caso, uma rotina de dispatch de driver) que é usado para ler os setores do disco para que quando as ferramentas (como, por exemplo, antivírus) tentarem ler o MBR, um MBR limpo seja apresentado às ferramentas em seu lugar. A novidade, no entanto, é que a técnica foi usada contra sistemas operacionais baseados em Windows NT. Este desenvolvimento em recursos de malware/rootkit simplesmente apresenta outro exemplo de adaptação de técnicas antigas para novos alvos.

```
cli
xor    bx, bx
mov    ss, bx
mov    sp, 78FEh, sp
mov    sp, 78FEh
push  ds
pushad
cld
mov    ds, bx
mov    si, 413h
sub    word ptr [si], 2
lodsw
shl    ax, 6
mov    es, ax
mov    si, 7C00h
xor    di, di
mov    cx, 100h
rep movsw
mov    dx, 202h
mov    cl, 61
mov    dx, 00h
mov    bx, di
int    13h
xor    bx, bx
nop
mov    eax, [bx+(13h*4)]
mov    es:nt13h_handler, e
mov    word ptr [bx+(13h*4)], e
mov    word ptr [bx+(13h*4)], e
push  es
```

Figura 66: Instruções Iniciais encontradas no código MBR do Mebroot, causando o sentimento nostálgico de ver os vírus de boot do passado.

³ <http://www2.gmer.net/mbr/>

Programas de Scareware e Antivírus Falsos

Os programas de scareware (classificados como cavalo-de-tróia-FraudTool) também foram destacados este ano, porque um grande número de usuários havia relatado casos de fraude por scam. O esquema envolve a exibição de mensagens falsas de erro ou mensagens de detecção de malware, e em seguida atraem o usuário para comprar a versão completa de uma ferramenta ou programa de segurança falsos para consertar estes problemas propositadamente identificados. O esquema normalmente começa com um usuário sendo redirecionado a Web sites que exibem essas mensagens falsas ou Web sites oferecendo download de software de segurança para varrer o sistema (que por sua vez exibirá as mensagens falsas). Além disso, o malware instalado no sistema também pode gerar essas mensagens falsas. Em dezembro de 2008, a Federal Trade Commission (FTC) emitiu um alerta aos clientes do FTC⁴ para o scam e tomou medidas legais⁵ contra alguns dos perpetradores. Uma forma de evitar este scam é saber em que fornecedores se deve confiar. Por exemplo, os clientes podem procurar os produtos que estão em teste por empresas famosas de testes de AV como AV-Comparatives, AV-Test, ICSA ou West Coast Labs. Uma busca rápida pelo nome do produto em questão também pode revelar se se trata de um scam.



Figura 67: Imagem Descoberta num Web Site Vendendo Software Antivírus Falso

Esperamos que esta categoria de malware continue a crescer em popularidade por ser tão eficaz. Por outro lado, a conscientização do usuário também aumentará à medida que cada vez mais desses scams sejam revelados.

⁴ <http://ftc.gov/bcp/edu/pubs/consumer/alerts/alt121.shtm>

⁵ <http://ftc.gov/opa/2008/12/winssoftware.shtm>

Ataques de Botnets e Injeção SQL

Como foi discutido na seção "Vulnerabilidades de Aplicativos da Web" deste relatório, assistimos ataques em massa de injeção SQL, parte deles atribuíveis ao botnet Asprox. Esta combinação de recurso de botnet mais ataque de injeção SQL ativou outro método de distribuição em massa de malware, em que um grande número de sites afetados se torna efetivamente um ponto de entrega. Além disto, esses ataques automáticos também destacaram o alto número de Web sites vulneráveis à injeção SQL e asseguram que as práticas de desenvolvimento⁶ têm pela frente um longo caminho para conseguir reduzir estes ataques.

```
40 53 25 25 ;DECLARE%%20@S%%
40 30 29 30 20VARCHAR(4000);
53 54 28 30 SET%%20@S=CAST(0
30 56 41 52 x%%5%%20AS%%20VAR
45 58 45 43 CHAR(4000));EXEC
28 01 88 28 (@S);-- ¼/0ê+0ê+
```

Figura 68: Parte de um Modelo de Ataque de Injeção SQL Usado pelo Asprox Botnet

Worms Autorun

Conforme mencionados em nosso relatório da metade do ano, devido à popularidade crescente dos dispositivos do tipo MP3, unidades externas e molduras de fotos digitais, os autores de malware continuam a aproveitar a oportunidade, usando-os como vetores de infecção. Um caso de perfil alto relatado⁷ em novembro de 2008 envolvia sistemas do governo federal que foram afetados por malware. A propagação através de unidades removíveis e aproveitando-se o recurso Autorun do Windows continua a ser uma das formas mais bem sucedidas de propagação. Manter políticas de controle de uso de dispositivos externos em sistemas corporativos e desativar os recursos de Autorun do Windows poderia ajudar a mitigar a infecção destes tipos de malware.



⁶ <http://msdn.microsoft.com/en-us/library/ms998271.aspx>

⁷ <http://blog.wired.com/defense/2008/11/army-bans-usb-d.html>

Malware que Objetiva Usuários de Jogos On-line

Finalmente, este ano, vimos também um surto no número de variáveis de malware que objetivam usuários de jogos on-line. Como vimos na tabela, das 20 famílias de malware mais predominantes em 2008, um cavalo-de-troia Infostealer que objetiva usuários de jogos on-line mantém a posição número 2. Impulsionados pela popularidade contínua dos jogos on-line com uma economia clandestina de ativos virtuais roubados, podemos esperar que no próximo ano não haverá queda na produção de novas variáveis de malware que objetivam usuários de jogos on-line.



Figura 69: Publicação no Site World of Warcraft Community em Dezembro de 19, 2008 (Origem da imagem: <http://www.worldofwarcraft.com/index.xml>)

© Copyright IBM Corporation 2009

IBM Global Services
Route 100
Somers, NY 10589
E.U.A.

Produzido nos Estados Unidos da América.
Janeiro de 2009
Todos os direitos reservados.

A IBM e o logotipo IBM são marcas comerciais ou marcas registradas da International Business Machines Corporation nos Estados Unidos, em outros países, ou ambos.

Internet Security Systems e X-Force são marcas comerciais ou marcas registradas da IBM Internet Security Systems, Inc. nos Estados Unidos, em outros países, ou ambos. Internet Security Systems, Inc. é uma subsidiária mundialmente conhecida da International Business Machines Corporation.

Windows é uma marca registrada da Microsoft Corporation nos Estados Unidos, em outros países, ou ambos.

Outros nomes de empresas, produtos ou serviços podem ser marcas registradas ou marcas de serviços de terceiros.

As referências, nesta publicação, a produtos ou serviços IBM, não implicam no fato da IBM pretender torná-los disponíveis em todos os países em que a empresa opera.