Relatório

# Relatório de Ameaças da McAfee: Primeiro trimestre de 2009

Por McAfee® Avert® Labs

# Sumário

O *Relatório de Ameaças da McAfee* traz para você as mais recentes estatísticas e análises sobre ameaças relacionadas a email e Web. Este relatório trimestral foi criado pelos pesquisadores do McAfee Avert Labs, cuja equipe mundial proporciona uma perspectiva única do cenário de ameaças — abrangendo desde consumidores a empresas e desde os Estados Unidos aos demais países do mundo. Junte-se a nós para examinarmos os principais problemas de segurança dos últimos três meses. Ao terminar aqui, você pode encontrar mais informações no McAfee Threat Center: http://www.mcafee.com/us/threat_center/default.asp ou www.trustedsource.org.

No primeiro trimestre de 2009, vimos muitas mudanças significativas no cenário de ameaças em comparação com o que vimos um ano atrás ou mesmo há alguns meses. Doze meses atrás, ninguém poderia prever que os volumes de spam cairiam, mas com o fechamento do provedor McColo em novembro de 2008, foi exatamente o que aconteceu. Os níveis de spam ainda estão 30% abaixo de seus níveis de pico e não vimos o aumento que historicamente costuma ocorrer em março. A questão não é *se* o spam voltará aos níveis anteriores, mas *quando* isso acontecerá. Existem dados relacionados à criação de redes de bots e zumbis novos que sugerem que esse momento pode chegar antes do que se imagina.

A criação de sites maliciosos está aumentando, bem como os sites que hospedam malware — com milhares de novos sites aparecendo diariamente. Novas formas de malware estão sendo criadas todo dia e este relatório detalha aquelas que mais predominaram.

O worm Conficker, oficialmente denominado W32/Conficker.worm, recebeu mais atenção do que qualquer ameaça de segurança na história recente. Este relatório proporciona uma perspectiva sobre essa atenção ser exagerada ou real. Também abordaremos ameaças que não recebem o mesmo nível de atenção da mídia, mas que podem ser até mesmo mais perigosas que outras mais populares.

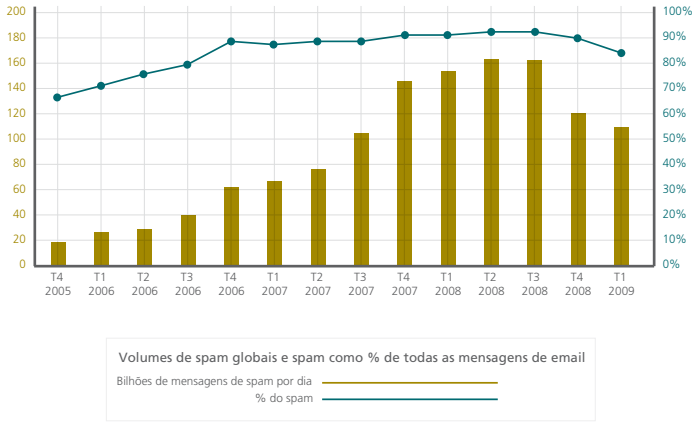
A geografia do cenário de ameaças continua a evoluir. Este relatório oferece análises das contribuições geográficas às ameaças — incluindo origem do spam, criação de zumbis e localização dos sites de malware, bem como identificação dos atores emergentes no negócio de criação de ameaças. O relatório também fornece alguns detalhes interessantes que sugerem que os países criadores de ameaças não se importam em utilizá-las contra entidades dentro de suas fronteiras.

Finalmente, voltamos nossa câmera para nós mesmos e damos uma olhada em algumas das previsões que fizemos em nosso *Relatório de previsões sobre ameaças em 2009*, publicado em janeiro, para ver se elas estão se concretizando ou como isso está acontecendo. Os destaques incluem o uso de eventos atuais e sites de rede social para propagar ameaças para usuários incautos.

## Spam: Ainda uma preocupação global

### Que recessão?

No geral, os volumes de email e spam no primeiro trimestre de 2009 estão em níveis não vistos há quase dois anos. Os remetentes de spam seguiram o restante da economia e sucumbiram ao panorama econômico difícil? A questão não é bem essa. O que está realmente acontecendo é que os níveis de spam ainda não se recuperaram totalmente do fechamento do provedor McColo, ocorrido em novembro de 2008. Em comparação com o mesmo trimestre do ano anterior, os volumes estão 20% menores em 2009 e 30% abaixo do terceiro trimestre de 2008, o qual teve os mais altos volumes trimestrais registrados até então. Os volumes de spam recuperaram-se em aproximadamente 70% desde que o hospedeiro de spam saiu do ar, mas ainda não atingiram seus níveis anteriores.



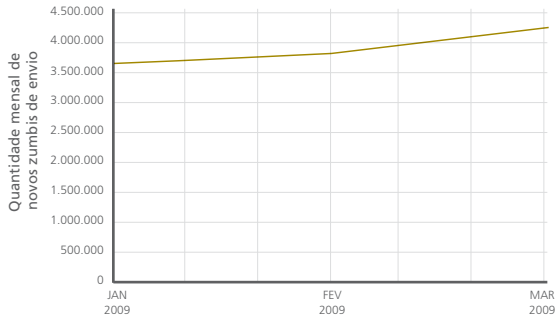

Nos últimos anos, o mês de março tem estabelecido recordes de volume de email, mas isso não se verificou este ano. No ano passado vimos uma média de 153 bilhões de mensagens por dia, enquanto este março teve uma média de apenas 100 bilhões de mensagens por dia.

O spam, como percentual do total de mensagens, caiu abaixo da marca de 90%, nível que não se via desde 2006. Em todo o ano de 2008, o spam representou 90% do volume total de mensagens de email, enquanto o último trimestre registrou apenas 86%. Embora as contas de email e sua atividade variem muito, estimamos que as pessoas estejam recebendo entre seis e doze emails a menos por dia em comparação com o ano passado.

Acreditamos que os volumes de spam voltarão a atingir os níveis de 2008, mas a capacidade dos remetentes de spam de reorganizar seus centros de comando e redes de bots após o fechamento levou mais tempo do que muitos previam quando o provedor foi tirado do ar. Enfim, para os remetentes de spam, isso é uma questão de retorno de investimento, como em qualquer outro negócio.

### Novos zumbis impulsionam a linha de produção

No último trimestre, detectamos quase doze milhões de novos endereços IP operando como "zumbis", ou seja, computadores sob o controle de remetentes de spam e outros. Isso representa um aumento significativo em relação aos níveis do último trimestre de 2008, quase 50%. O terceiro trimestre de 2008 também alcançou um número recorde de novos zumbis, mas foi superado neste trimestre em um milhão. Embora os volumes de spam ainda não tenham se recuperado do fechamento do provedor McColo, o nível de atividade dos novos zumbis indica que os remetentes de spam estão trabalhando duro para recuperar a infra-estrutura perdida e que os volumes voltarão em breve aos níveis anteriores.




Podemos dividir por país os sistemas infectados. No último trimestre, 63% dos novos zumbis foram contabilizados nos dez principais países. Esse valor representa uma pequena diminuição em relação aos dois trimestres anteriores. Parece que os remetentes de spam estão recorrendo a máquinas de mais países para impulsionar seu negócio.

| T1 2009 | | T4 2008 | | T3 2008 | |
|---|---|---|---|---|---|
| **País** | **Percentual de IPs** | **País** | **Percentual de IPs** | **País** | **Percentual de IPs** |
| Estados Unidos | 18,0 | China | 15,8 | China | 20,4 |
| China | 13,4 | Estados Unidos | 15,4 | Estados Unidos | 16,5 |
| Austrália | 6,3 | Alemanha | 6,5 | Alemanha | 6,8 |
| Alemanha | 5,3 | Reino Unido | 6,0 | Reino Unido | 6,0 |
| Reino Unido | 4,7 | Brasil | 4,9 | Brasil | 4,8 |
| Brasil | 4,0 | Espanha | 4,3 | Espanha | 3,7 |
| Índia | 3,1 | Austrália | 4,1 | Índia | 2,5 |
| Espanha | 3,0 | Itália | 3,5 | Rússia | 2,4 |
| Coréia do Sul | 2,8 | Rússia | 3,1 | Coréia do Sul | 2,4 |
| Rússia | 2,5 | Coréia do Sul | 2,4 | Itália | 2,2 |
| | | | | | |
| **Total** | **63,3** | **Total** | **66,0** | **Total** | **67,5** |

China e Estados Unidos têm disputado a posição de maior destaque nos últimos três trimestres e predominam em número de máquinas zumbis sob controle dos remetentes de spam. Um caso notável é a Austrália, que deixou de integrar a lista dos dez principais países no terceiro trimestre de 2008. Em dois trimestres, ela subiu vertiginosamente para o terceiro lugar, representando 6% de todos os novos zumbis. As terras australianas estão mostrando que são um terreno fértil para o recrutamento de zumbis.

| T1 2009 | | T4 2008 | |
|---|---|---|---|
| **País** | **% do total** | **País** | **% do total** |
| Estados Unidos | 35,0 | Estados Unidos | 34,3 |
| Brasil | 7,3 | Brasil | 6,5 |
| Índia | 6,9 | China | 4,8 |
| Coréia do Sul | 4,7 | Índia | 4,2 |
| China | 3,6 | Rússia | 4,2 |
| Rússia | 3,4 | Turquia | 3,8 |
| Turquia | 3,2 | Coréia do Sul | 3,7 |
| Tailândia | 2,1 | Espanha | 2,4 |
| Romênia | 2,0 | Reino Unido | 2,3 |
| Polônia | 1,8 | Colômbia | 2,0 |
| | | | |
| | **70,0** | | **68,3** |

Spam por país: Estados Unidos, novamente um líder mundial

Os fabricantes de automóveis dos EUA podem estar com problemas de fabricação e vendas, mas os remetentes de spam dos Estados Unidos continuam na liderança mundial, representando 35% de toda a produção de spam global. Embora as operações de comando e controle sejam uma infra-estrutura internacional, os remetentes de spam ainda preferem utilizar computadores dos Estados Unidos para produzir spam. Os dez principais países dominam a produção de spam, contribuindo com quase 70% do total e superando largamente os mais de 200 outros países do mundo.

Observando os dois últimos trimestres, vemos que a Índia apresentou o maior aumento percentual, passando a contribuir com quase 7% do spam global. Sua produção de spam dobrou em relação ao trimestre anterior. Talvez o spam seja a mais recente indústria a experimentar a terceirização para a Índia.

Tailândia, Romênia e Polônia também são recém-chegadas à lista dos dez principais. Esses dados corroboram a idéia de que os remetentes de spam estão procurando por toda parte novos lugares de onde lançar seu spam.

| T1 2009 | | T4 2008 | | T3 2008 | |
|---|---|---|---|---|---|
| Venda de remédios que exigem receita médica | 25,0 | Venda de remédios que exigem receita médica | 37,0 | Melhoria do desempenho sexual masculino | 31,2 |
| Anúncios | 21,9 | Anúncios | 19,3 | Anúncios | 19,3 |
| Réplicas de produtos | 18,8 | Melhoria do desempenho sexual masculino | 16,8 | Venda de remédios que exigem receita médica | 10,7 |
| Melhoria do desempenho sexual masculino | 17,5 | DSN | 9,5 | Storm | 8,0 |
| DSN | 7,1 | Encontros | 3,9 | DSN | 7,7 |
| Storm | 1,6 | Réplicas de produtos | 2,6 | Últimas notícias | 6,7 |
| Diplomas | 1,1 | Empregos | 1,7 | Réplicas de produtos | 6,0 |
| Software | 1,1 | Software | 1,5 | Empréstimos para quitação de dívidas | 1,6 |
| Empréstimos para quitação de dívidas | 1,0 | Empréstimos para quitação de dívidas | 1,2 | Operações bancárias | 1,1 |
| Outros | 4,9 | Outros | 6,5 | Outros | 7,7 |
| | **100,0** | | **100,0** | | **100,0** |

Spam por tipo: sexo, drogas e muito mais

As mensagens de spam voltadas para a melhoria do desempenho sexual masculino, venda de remédios que exigem receita médica e anúncios em geral continuam entre os principais tipos de spam enviados. Esses três tipos, somente, representam aproximadamente 60% do spam enviado durante os últimos três trimestres. Parece que o dito cultural "sexo, drogas e rock'n'roll" continua valendo no spam. Pelo menos quase. Talvez tenhamos amadurecido um pouco. Hoje, a frase poderia ser "sexo, drogas e dinheiro".

O spam de réplica de produtos (principalmente relógios falsificados) subiu bastante neste trimestre, contribuindo com quase 19% do total de spam. Esse tipo de spam de réplicas foi popular no ano passado, mas também apresentou um crescimento significativo neste trimestre. Isso sugere que, em momentos econômicos difíceis, os remetentes de spam estão nos ajudando a aumentar nosso poder de compra encontrando boas pechinchas em liqüidações baratas.

O spam de notificação de status de entrega de mensagens continua firme em 8% do total de spam. Essas mensagens estão quase sempre associadas a ataques de phishing e ocorrem como uma aparente notificação de mensagem não entregue ao destinatário após o endereço de email da vítima ser alvo de spoof. Isso deixa claro que o phishing continua vivo, e bem. Muitas dessas mensagens estão relacionadas a finanças, sendo uma tentativa de obtenção de informações pessoais.

### Os remetentes de spam não respeitam a soberania de país algum — nem mesmo de seu próprio país

Há um mito na comunidade de cibersegurança de que os criminosos on-line (dos quais um número significativo residiria na Europa Oriental) preferem concentrar-se em alvos de países ocidentais e evitam atacar pessoas ou empresas de jurisdição local. Estamos começando a ver indícios que derrubam

esse mito. A Internet ignora fronteiras geográficas. Agora está claro que os cibercriminosos aproveitam qualquer oportunidade que encontram. Temos visto evidências de que cibercriminosos comprometeram profundamente algumas importantes corporações e agências governamentais da Rússia e da Europa Oriental, bem como altos funcionários dessas entidades.

O TrustedSource™ da McAfee observou recentemente emails e spams carregados de malware oriundos de uma variedade de agências governamentais e instituições bancárias da Rússia. De acordo com nossa análise, os bancos russos comprometidos são:

- Rusfinance Bank
- OGO Bank
- Tusarbank
- Link Capital Investment Bank
- The Maritime Bank
- Vladivostok Alfa Bank
- Bank Eurotreid
- Bank Voronezh
- Bashcreditbank
- Enisey's United Bank
- Inter-Svayz Bank

Nossos dados também sugerem que os sistemas de computadores dos seguintes órgãos governamentais russos são controlados por cibergangues:

- Ministério da Receita, região de Nazran
- Rede de Internet Estatal Russa
- Instituto Regional de Finanças e Economia
- Instituto Conjunto de Pesquisa Nuclear
- Centro Médico do Gabinete do Presidente da Federação Russa
- Fundo de Pensão da Federação Russa
- Rede pessoal do Poder Judiciário da Federação Russa
- JSC, Comunicação Celular da Chechênia

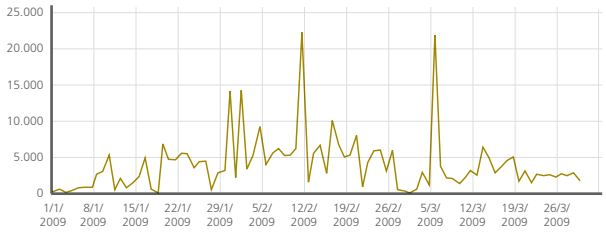
Esses dados da Rússia sugerem que os criminosos on-line escolhem indiscriminadamente seus alvos e atacam qualquer organização que seja de interesse financeiro ou atraente de alguma outra forma. Embora a Rússia lidere indiscutivelmente nesse tipo de atividade (e no próprio volume de spam que produz), nossa análise mostra o mesmo tipo de atividade em outros países da antiga União Soviética, como Ucrânia, Belarus, Armênia, Azerbaijão, Geórgia, Cazaquistão, Quirguistão, Moldávia, Tadjiquistão, Turcomenistão e Uzbequistão.

## Web: Novos sites com reputações maliciosas aparecem diariamente

Ao longo deste trimestre, vimos a continuidade de muitas das ameaças que se apresentaram durante o último trimestre de 2008 — mas com maior intensidade. Embora a maior parte do alarde e da atenção da mídia tenha se voltado para o Conficker, este não foi, de maneira alguma, a única ameaça a prevalecer durante este trimestre. Mesmo desconsiderando a atividade do Conficker, ainda assim tivemos um leve aumento de atividade de um ano para outro e um nítido aumento em relação aos trimestres anteriores. Os aplicativos antivírus enganosos foram um problema que causou uma certa preocupação na Web, além do aumento nas atividades de phishing e fraudes.

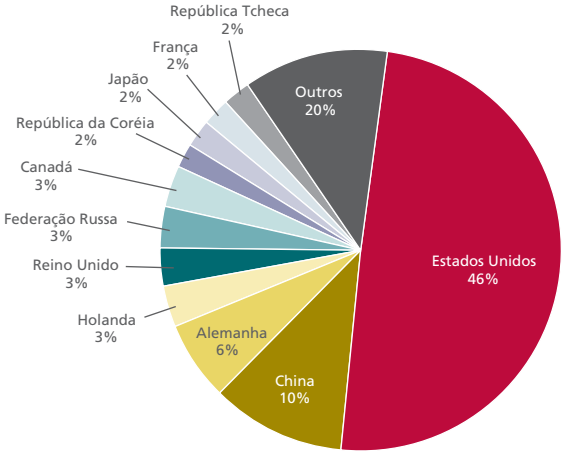
Os domínios maliciosos que o Conficker contactaria não foram incluídos em nenhum dos gráficos desta seção, exceto pelo gráfico "Distribuição de sites com reputações maliciosas". Embora os dados do Conficker sejam uma parte importante do panorama de ameaças, eles diluem o conjunto de atividades maliciosas. Existem muitas outras ameaças que estão se tornando mais predominantes. Os golpistas e autores de malware estão se aproveitando das incertezas econômicas e de nossas aflições para levar adiante uma variedade de sites de fraudes. Suas jogadas incluem sites para evitar execução de hipotecas e sites de phishing sobre praticamente qualquer coisa; eles até oferecem cartões de descontos

em lojas. Os sites antivírus enganosos continuam a vitimar usuários incautos. Os métodos para atrair os usuários aos sites continuam a evoluir. Mesmo desconsiderando toda a atividade do Conficker, o número de URLs que cruzaram a linha dos níveis de reputação "maliciosos" (ou "vermelhos") aumentou perceptivelmente em comparação com os dois últimos trimestres de 2008.




Quantidade diária de novos sites com reputações maliciosas

Onde estão localizados esses URLs com má reputação na Web? Não onde a maioria das pessoas pensa.



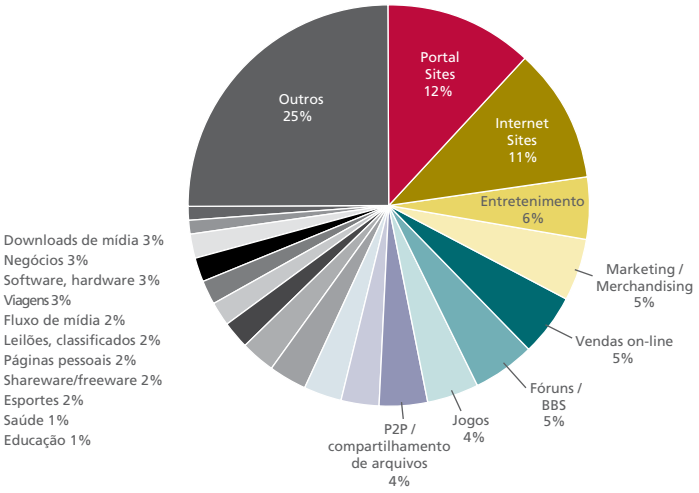

Distribuição de sites com reputações maliciosas

Por que a mudança súbita no que muitos consideravam a "norma" (a tríade Estados Unidos, China e Rússia) em relação a atividades maliciosas na Web?[1] Isso não significa que alguns desses países tiveram menos URLs com reputação maliciosa. Em vez disso, vimos um crescimento maior em outros países. Muito desse crescimento tem relação com os lugares onde o Conficker hospedou alguns domínios que planejava contactar ou que tinha contactado. Na verdade, a contribuição do Conficker bastou para levar a Holanda a um empate pela quarta colocação. Embora a Holanda seja há muito tempo uma favorita na hospedagem de URLs de phishing, o Conficker promoveu um salto significativo em sites infectados por malware e outros conteúdos maliciosos. No entanto, essa mudança não pode ser inteiramente atribuída ao Conficker. O Canadá subiu para a lista dos 10 maiores em hospedagem de servidores Web maliciosos devido à variedade de malware e spyware disponibilizada por esses sites.

Uma constatação importante é que esses mesmos países aparecem em vários vetores de ataque — sites maliciosos, sites que hospedam spyware/adware, phishing e spam. Os sete principais países que hospedam sites com reputação maliciosa estão entre os dez principais que hospedam sites de phishing, spam e malware/spyware.

1. No terceiro trimestre de 2008, o ranking era EUA com 41%, China com 12%, Rússia com 7%, Alemanha e Holanda com 5% cada, Coréia do Sul com 4%, Hong Kong com 3%, Taiwan, Canadá e República Tcheca com 2% cada e os demais países com 17%.

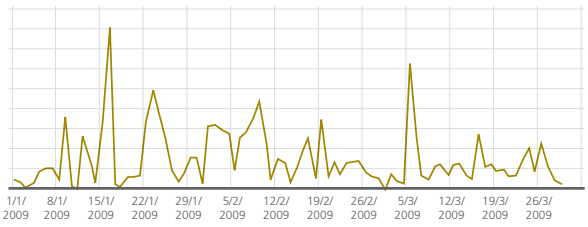
Os sites com reputação maliciosa variam consideravelmente em seus objetivos, sejam legítimos, duvidosos ou fraudulentos. Você ainda corre um risco maior ao visitar um site de pornografia ou de apostas que não esteja associado a uma empresa reconhecida e legítima. No entanto, qualquer site é vulnerável e qualquer tipo de conteúdo que um usuário possa querer acessar é uma oportunidade para os distribuidores de malware explorarem.




20 principais categorias legítimas consideradas com reputação de 'site malicioso' pelo TrustedSource

Neste trimestre, os servidores de conteúdo tiveram um aumento de popularidade junto aos distribuidores de malware como ferramenta para conteúdo malicioso e ilegal. Já vimos essa tendência entre sites estabelecidos e administrados por provedores idôneos e altamente respeitados, bem como naqueles menos conhecidos e mais questionáveis. A combinação dessa ameaça com o uso difundido de blogs e otimização de mecanismos de pesquisa é mais crítica do que nunca para que todo computador tenha plena segurança na Web.

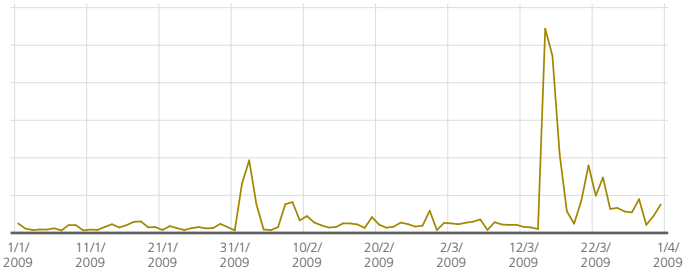
Tratamos do *onde*; agora vamos discutir os *tipos* de ameaças que vimos. Além do Conficker, tivemos um trimestre atribulado em termos de novas explorações e malware disponíveis na Web.




Novos sites que fornecem malware e PUPs

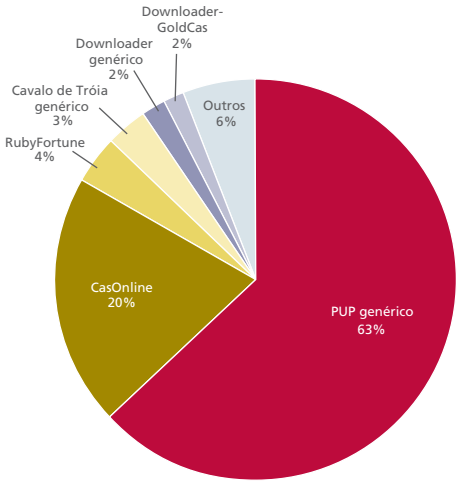
O gráfico acima mostra uma ilustração do número de sites que fornecem malware e programas potencialmente indesejados (PUPs) que foram detectados neste trimestre pela rede TrustedSource da McAfee. (O gráfico mostra sites que realmente hospedam malware, refletindo o tráfego de usuários para esses sites. Não estão incluídos sites legítimos que são explorados para direcionar usuários para sites com malware. Além disso, neste gráfico removemos nossa pesquisa proativa para proporcionar uma visão verdadeira das novas e exclusivas ameaças disponíveis durante uma navegação padrão, seja na escola, no trabalho ou em casa.)

Por outro lado, os gráficos abaixo ilustram o que a nossa metodologia proativa descobriu em relação a novos e exclusivos downloads de malware que estavam sendo servidos por vários sites. Tivemos alguns picos interessantes decorrentes de novas explorações ou quando encontramos "minas de ouro" de downloads maliciosos e PUPs.




Downloads de malware e PUPs, identificados proativamente por dia

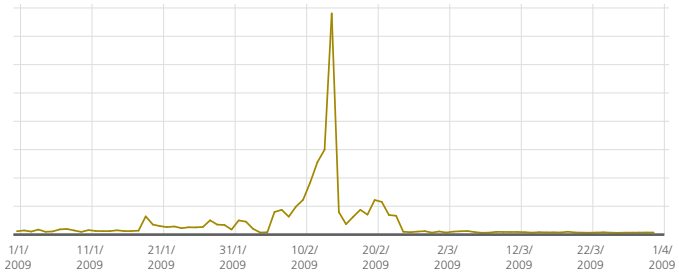
Nossas observações proativas — perscrutações ("crawling") e verificações regulares de sites, além de métodos exclusivos de mineração para obtenção de informações maliciosas adicionais – mostraram um pico expressivo em novos downloads de malware relacionados a cassinos por volta do final do mês de janeiro e início de fevereiro, bem como um pico em PUPs genéricos por volta do final do trimestre. Essa atividade considerou os quatro principais tipos de download de malware durante o trimestre. (Consulte o gráfico seguinte). Outro malware de interesse é a presença contínua do cavalo de Tróia Vundo, que se tornou mais ativo nos últimos três meses.




Predomínio de downloads de malware e PUPs, por tipo

Uma das ameaças amórficas da Web que enfrentamos é a *exploração (exploit)*, um termo que pode significar muitas coisas, freqüentemente diferentes, para pesquisadores e usuários. O Avert Labs rastreia novas páginas que hospedam explorações de navegador à medida que perscruta e monitora a Web, além de identificar regularmente novas vulnerabilidades de segurança em navegadores. Quando os navegadores (e seus plug-ins) não são mantidos atualizados, eles podem se tornar o parque de diversões dos autores de malware. Uma vez que o autor se torna o dono do pedaço, o computador do usuário pode receber códigos de programação que permitam infecções por adware, espionagem dos pressionamentos de teclas e outras atividades maliciosas.

*Quando os navegadores (e seus plug-ins) não são mantidos atualizados, eles podem se tornar o parque de diversões dos autores de malware.*

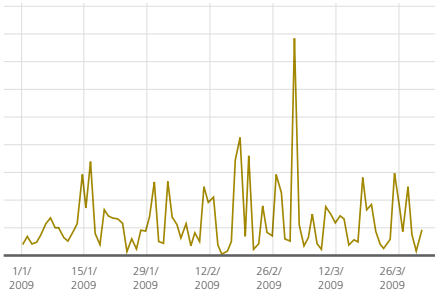



Sites descobertos hospedando explorações de navegador

## Atividade de anonimização

Os autores de malware estão incrementando sua utilização de ataques de URL redirecionado, seja através de um anonimizador ou de uma interface Web 2.0 utilizando um servidor de conteúdo. Pode ser para evitarem detecção padrão (atuando como um URL incorporado em vez de um URL de origem) ou para se beneficiarem da reputação do site que parece fornecer o malware.

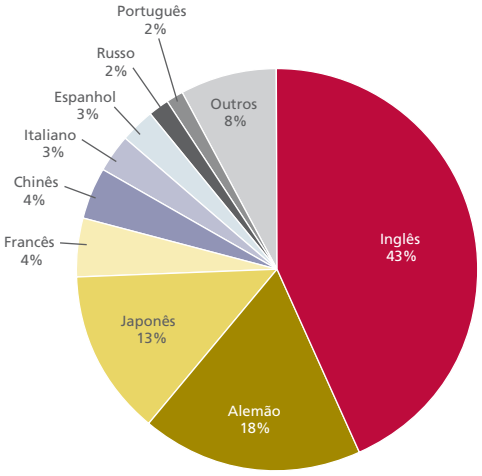
Um anonimizador é uma ferramenta que oculta a identidade de um usuário enquanto este está on-line. A maioria dos anonimizadores não é maliciosa e, portanto, não está incluída em nossas discussões anteriores sobre riscos de segurança. No entanto, sua utilização pode abrir a porta para um ataque "man in the middle", no qual um anonimizador malicioso ou seqüestrado injeta código nas mensagens que trafegam, numa direção ou noutra, entre o usuário e o servidor. Isso não apenas coloca o usuário em risco, mas também expõe hosts e redes que, de outra forma, estariam protegidos. No geral, a atividade dos anonimizadores aumentou neste trimestre em comparação com o anterior. Houve também um leve aumento na atividade de um ano para outro, neste trimestre.




Novos anonimizadores por dia

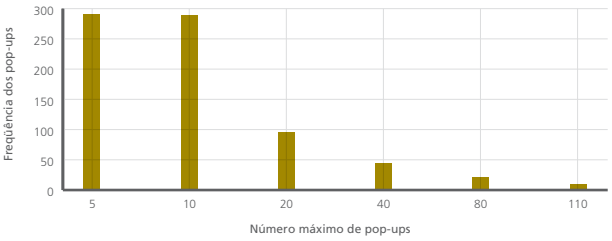
## Tendências gerais da Web

A Web é uma comunidade global. Basta observar as conexões em qualquer site de rede social ou profissional. As páginas da Web continuam surgindo em um ritmo constante para incluir mais idiomas. Os mesmos ataques de blog que aparecem em sites de alto perfil nos Estados Unidos também são distribuídos através de blogs chineses, brasileiros e de muitos outros países. Os ataques de hoje empregam uma rede disseminada. Além disso, quando os distribuidores de malware tiram proveito da notoriedade de marcas (como eventos esportivos de renome e o uso de malware incorporado em tabelas de campeonatos e em JPGs de jogadores), eles estão utilizando marcas globais para atingir públicos em todos os idiomas.




Distribuição de idiomas no conteúdo da Web

O incômodo causado pelas telas pop-up não diminuiu. É interessante observar que, apesar dos bloqueadores de pop-up e de ferramentas semelhantes, a maioria dos sites continua recorrendo a esse artifício. O número máximo de pop-ups que vimos em um mesmo site foi 116.




Distribuidor de pop-ups em sites com pelo menos cinco

Continuamos a ver o uso disseminado de URLs legítimos relacionados a empresas e Web 2.0 para disseminação de malware. Há dez anos ou mais, parecia possível permanecer a salvo simplesmente ficando longe de determinados conteúdos, mas hoje as ameaças parecem nos encontrar, independente de onde estejamos navegando. Qualquer site que possa ser explorado (através de qualquer das várias vulnerabilidades) certamente o será. Os administradores vêem rotineiramente varreduras com o objetivo de explorar seus servidores. O que é interessante é o alto predomínio dessas varreduras vindas de sites e servidores associados a todo tipo de coisa, como software ilegal, sites maliciosos e anonimizadores. Se um site de grande tráfego está vulnerável, a questão não é se ele será explorado, mas quando.

*As empresas na Web precisam ser tratadas com os mesmos critérios que seriam aplicados a um vendedor de porta em porta.*

Vimos um aumento marcante nas fraudes na Web. É de se esperar que isso aumente, uma vez que os perpetradores das fraudes se valem dos receios da população global através dos emails de spam e da Web. Costuma ser difícil determinar se uma organização é legítima. As empresas na Web precisam ser tratadas com os mesmos critérios que seriam aplicados a um vendedor de porta em porta. Os usuários precisam saber que após fornecer informações de cartão de crédito a um fraudador para uma doação on-line ou serviço falsificado, esses dados estão perdidos.

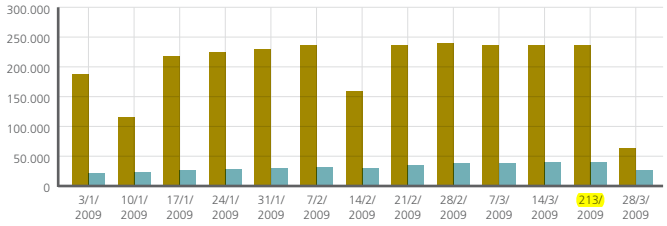
No entanto, nossa pesquisa mostra alguma esperança para a economia. Os sites imobiliários tiveram um crescimento marcante neste trimestre, chegando às dez principais categorias de conteúdo disponível para os usuários (e empurrando os esportes para fora do grupo dos principais).

## Malware: Exagero do Conficker x realidades do AutoRun

Os últimos meses foram repletos de histórias sobre o Conficker. Parecia que era a única ameaça com a qual valia a pena se preocupar. No entanto, quando examinamos os números, vemos um cenário diferente. O Conficker não é exatamente o final dos tempos.

Ele foi, com certeza, um importante elemento de malware por vários motivos. Ele infectou inúmeros hosts. Ele foi ativamente desenvolvido, mantido e discutido. No entanto, o número real de detecções não foi tão grande quanto se poderia supor de um malware que chamou tanta atenção.

Por outro lado, vimos neste trimestre exemplos de malware preocupantes. A história é outra com o malware baseado em AutoRun, que utiliza predominantemente unidades USB ou memória flash para se replicar e que foi visto em números bem maiores que o Conficker neste trimestre. Vejamos ambos lado a lado:



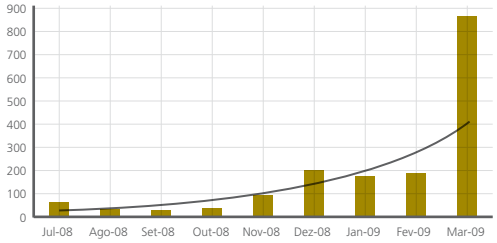

Nos últimos 30 dias, menos de 10% de todas as detecções reportadas foram worms AutoRun. O Conficker começou com aproximadamente 1% e aumentou 12 vezes, mas ainda representa menos de 15% do pico de detecções de worms AutoRun.

## Atualização de previsões

No início deste ano, o McAfee Avert Labs lançou suas *Previsões sobre ameaças em 2009.*[2] Várias de nossas estimativas se concretizaram neste trimestre.

### Fogo amigo resulta em baixas

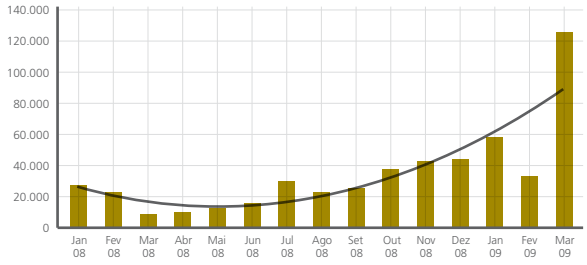
Ao longo da última década, o popular vetor de ameaças caracterizado pelo recebimento de vírus de amigos ficou quase totalmente para trás. No entanto, a Web 2.0 revitalizou esse velho método de ataque. Durante este trimestre, variantes do Koobface pegaram milhares de usuários de surpresa quando estes receberam o vírus de amigos no Facebook. Sem conhecimento das vítimas, os links associados às mensagens enviadas pelo vírus levavam a sites que distribuíam o worm. Logo em seguida, os computadores contraíam o vírus e enviavam mensagens infectadas para o círculo de amigos do usuário. As redes sociais continuam a oferecer aos atacantes um vetor popular para ataques de engenharia social.




2. McAfee Avert Labs Threat Center. http://www.mcafee.com/us/local_content/reports/2009_threat_predictions_report_br.pdf

### Falsa World Wide Web

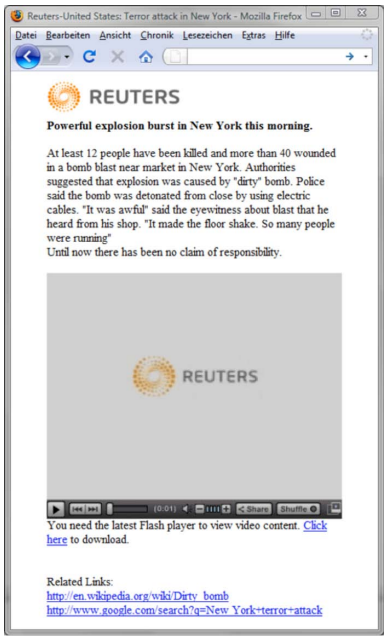
Em fevereiro, o Facebook foi explorado por atacantes que criaram aplicativos falsos utilizando a plataforma Facebook. Muitos usuários morderam a isca e instalaram esses aplicativos. Os eventos chamaram a atenção da mídia, o que levou o McAfee Avert Labs a expor uma enorme quadrilha de otimização de mecanismos de pesquisa que tinha como alvo as principais palavras pesquisadas no Google. Os atacantes não apenas roubavam materiais de copyright de sites populares, como também se aproveitavam de outros sites populares, como o Democrats.org, para ajudar a levantar seus índices no Google. O objetivo dos atacantes com a otimização de resultados de pesquisas era instalar software antivírus falsificado. Foi o caso de um aplicativo falso de Facebook, levando a resultados de pesquisa falsos e a software de segurança falso. Esses incidentes exemplificam a necessidade dos usuários navegarem com segurança.




Binários exclusivos de falsos programas antivírus descobertos

### Ameaças que falam a sua língua

Os atacantes sabem que quanto mais relevante e contextualizado for um ataque, maiores as possibilidades de que uma pessoa faça algo: clicar em um link, digitar um nome de usuário e senha ou instalar um aplicativo. Histórias sobre eventos ocorridos em nossa vizinhança têm mais chances de nos chamar a atenção do que a mesma coisa ocorrida no outro lado do mundo. Em fevereiro e março, os indivíduos por trás do vírus Waledac exploraram esse conceito. Vítimas incautas foram atraídas para sites personalizados com base em sua localização geográfica, dando uma impressão de autenticidade. Enquanto os usuários liam "notícias locais", o site tentava instalar furtivamente o vírus através de um código de exploração que infectava o usuário de passagem pelo site.




## Blog do McAfee Avert Labs

### Google e o abuso do mecanismo de pesquisa

Google. O nome, sozinho, significa muitas coisas diferentes para muitas pessoas diferentes. Para pessoas à procura de emprego, é uma maneira de encontrar as ofertas mais recentes. Para empregadores, é uma maneira de encontrar pessoas qualificadas on-line. Para consumidores, é uma ferramenta eficaz para encontrar preços atraentes pelos bens que se procura. Para criadores de malware e cibercriminosos, é uma ferramenta cada vez mais eficaz para distribuir malware e entrar para o cibercrime. Quando se leva em conta o que os mecanismos de pesquisa representam em termos de atividade de Internet nos dias de hoje, nada mais lógico que os criadores de malware procurem tirar proveito desse poder como uma maneira de distribuir suas criações. Para uma amostra de nossos blogs sobre esse assunto, dê uma olhada nas seguintes entradas do blog da McAfee Avert:

- http://www.avertlabs.com/research/blog/index.php/2009/03/15/democratsorg-cans-the-spam/
- http://www.avertlabs.com/research/blog/index.php/2009/03/10/democratsorg-blog-spam-contributes-to-google-search-poisoning/
- http://www.avertlabs.com/research/blog/index.php/2009/02/27/google-bucking-the-trend/
- http://www.avertlabs.com/research/blog/index.php/2009/02/25/google-trends-abused-to-serve-malware/
- http://www.avertlabs.com/research/blog/index.php/2009/01/07/google-code-project-abused-by-spammers/
- http://www.avertlabs.com/research/blog/index.php/2009/01/17/do-not-worry-obama-di-not-refuse-to-be-a-president/

Considerando o poder combinado da indexação e de palavras-chave populares com o incentivo do dinheiro fácil para os cibercriminosos, é de se esperar que esse tipo de abuso continue.

### A economia e o medo

Os problemas econômicos globais continuam a preocupar muitas pessoas. Questões de segurança e terror continuam a afligir outras. Os criadores de malware e cibercriminosos podem facilmente transformar esses receios em lucro. Essa tendência econômica, que foi uma de nossas previsões sobre ameaças para 2009, foi certamente aproveitada ao longo deste trimestre de muitas maneiras preocupantes. O medo é um motivador poderoso quando utilizado como isca de engenharia social por cibercriminosos:

- http://www.avertlabs.com/research/blog/index.php/2009/03/16/breaking-news-waledac-terror-attack-in-a-city-near-you/
- http://www.avertlabs.com/research/blog/index.php/2009/02/23/malware-riding-on-the-tides-of-the-economic-crisis/
- http://www.avertlabs.com/research/blog/index.php/2009/02/06/cybercrime-online-threats-and-the-recession/
- http://www.avertlabs.com/research/blog/index.php/2009/01/05/one-hacker-may-conceal-another/
- http://www.avertlabs.com/research/blog/index.php/2009/01/20/fake-antivirus-and-a-real-threat/
- http://www.avertlabs.com/research/blog/index.php/2009/01/29/hoax-or-not-treat-it-the-same/

Fraudes, spam e phishing funcionam muito bem em bons tempos, e melhor ainda em tempos difíceis. Lembre-se sempre de que os malfeitores lêem as mesmas notícias que nós e que eles utilizam manchetes e eventos contra nós, a menos que permaneçamos atentos.

## Sobre o McAfee Avert Labs

McAfee Avert Labs é a equipe de pesquisa global da McAfee, Inc. Com equipes de pesquisa voltadas para malware, programas potencialmente indesejados, intrusões de host, intrusões de rede, malware móvel e divulgação de vulnerabilidade ética, o Avert Labs desfruta de uma visão ampla da segurança. Essa visão expandida permite que os pesquisadores da McAfee aprimorem continuamente as tecnologias de segurança e protejam melhor o público.

## Sobre a McAfee, Inc.

A McAfee, Inc., sediada em Santa Clara, Califórnia, é a maior empresa do mundo dedicada à tecnologia de segurança. Totalmente comprometida em combater os rigorosos desafios de segurança globais, a McAfee provê soluções proativas e com qualidade comprovada e serviços que ajudam a manter sistemas e redes protegidos mundialmente, permitindo aos usuários conectarem-se à Internet, navegarem e realizarem compras pela Web com segurança. Apoiada por uma equipe de pesquisas premiada, a McAfee desenvolve produtos inovadores que capacitam os usuários domésticos, as empresas dos setores público e privado e os provedores de serviços, permitindo-lhes manter a conformidade com as regulamentações de mercado, proteger dados, prever interrupções, identificar vulnerabilidades e monitorar continuamente, além de incrementar a segurança em TI. http://www.mcafee.com.br.

McAfee®

McAfee do Brasil
Comércio de Software Ltda.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070, São Paulo - SP
Brasil
www.mcafee.com.br



5395rpt_avert_quarterly-threat_0409