Relatório

Relatório da McAfee sobre Ameaças: Segundo trimestre de 2009

Por McAfee® Avert® Labs

Sumário

O Relatório da McAfee sobre Ameaças traz para você as mais recentes estatísticas e análises sobre ameaças relacionadas a e-mail 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.[1] Você também encontrará nosso relatório sobre ameaças do primeiro trimestre.[2]

No segundo trimestre de 2009, vimos a produção de spam recuperar-se rapidamente de um recente revés e crescer até níveis recordes. Os zumbis (computadores sequestrados por remetentes de spam para o envio de mensagens) também quebraram recordes. Nós categorizamos a produção de spam por país e por assunto.

Na Web, o malware continua a explorar os navegadores, tanto em sites legítimos quanto maliciosos. Redes de robôs "capturam" e controlam máquinas para roubar dados e enviar spam. O Twitter tornou-se um alvo popular para os atacantes. É a atual menina dos olhos entre as ferramentas de rede social e os autores de malware estão plenamente cientes do seu potencial para abuso. Você sabe que o seu novo estilo de vida on-line está fazendo sucesso quando ele está programado para um "Month of Twitter Bugs" (mês dos bugs do Twitter). O Twitter também desempenhou um papel "hacktivista" na eleição iraniana e em seus desdobramentos.

No mundo do malware, vimos um rápido crescimento nos cavalos de Tróia para roubo de senhas, os quais visam, principalmente, os seus dados bancários. Esses programas são simples, furtivos e, agora, mais fáceis do que nunca de produzir. Sites hospedados principalmente na Rússia oferecem ferramentas para criação de cavalos de Tróia que permitem a atacantes novatos adquirir os meios de roubar os seus dados. O malware de AutoRun também é fácil de criar, graças à ampla disponibilidade de compiladores e empacotadores de freeware.

O spam volta com força total

Se a economia pudesse se recuperar como o spam fez no segundo trimestre, estaríamos todos muito mais satisfeitos com nossas contas de aposentadoria. Houve um surto de spam desde o trimestre anterior, com um aumento de quase 80%. O spam no trimestre passado caiu drasticamente em relação aos trimestres anteriores, em grande parte devido ao fechamento do provedor McColo. Mesmo assim, o surto deste trimestre é significativo e atingiu níveis recordes. O período anterior no qual medimos um aumento recorde foi o segundo trimestre de 2008, mas o trimestre atual o superou em 10%. Em nosso *relatório sobre spam de julho*, informamos que os novos zumbis criados no primeiro trimestre seriam um importante indicador do que estava por vir, e essa previsão se comprovou.[3]

A atividade de spam, apenas no mês de junho, merece menção especial. Em junho foi produzida a maior quantidade de spam já vista, superando o último mês de pico, outubro de 2008, em mais de 20%.

O spam como uma porcentagem do total de e-mail também atingiu um recorde neste trimestre. Estimamos seu predomínio em 92%. Isso excede os 91% registrados no segundo e terceiro trimestres do ano passado.

Portanto, talvez o spam seja o principal indicador econômico e de que tempos melhores estão logo à frente. Esperamos que isso seja verdade, mas uma coisa podemos prever: o spam está de volta e parece disposto a atingir níveis sem precedentes.

1 http://www.mcafee.com/us/threat_center/default.asp ou www.trustedsource.org
2 McAfee Avert Labs, *Relatório da McAfee sobre Ameaças: Primeiro trimestre de 2009*. http://img.en25.com/Web/McAfee/5395rpt_avert_quarterly-threat_0409ptbr_s_fnl.pdf
3 http://www.mcafee.com/us/local_content/reports/mcafee_spam_report_july09.pdf

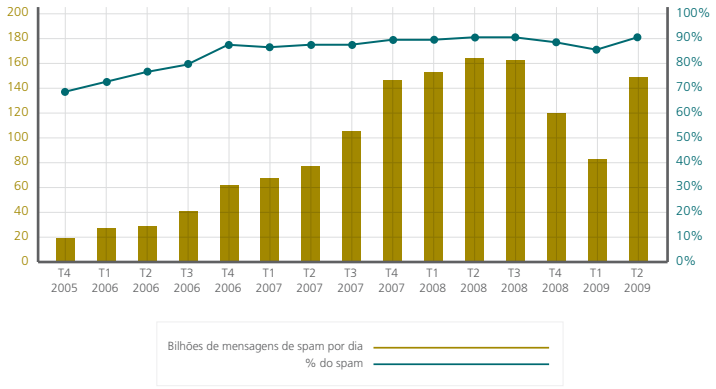


Figura 1: Volumes de spam globais e spam como porcentagem de todas as mensagens de e-mail

Novos zumbis

Observamos quase catorze milhões de novos zumbis neste trimestre. Trata-se de mais um recorde, superando o recorde do último trimestre, no qual vimos quase doze milhões de novos zumbis entrarem em ação. Isso significa um aumento de mais de 150.000 novos zumbis por dia, sistemas que têm o potencial de enviar spam e outros itens maliciosos para o seu computador. Com esse tipo de tendência de criação de zumbis em andamento, é fácil prever que os volumes de spam subirão no próximo trimestre.

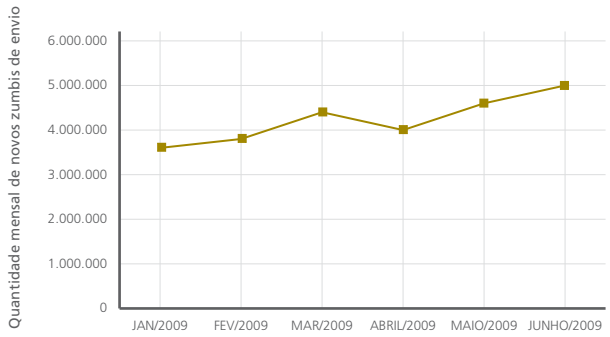


Figura 2: Novos zumbis remetentes de spam, por mês.

Novos zumbis por país

Examinando a produção de zumbis por país, vemos que os suspeitos de sempre perfazem nossos 10 principais países. O único país a entrar no clube neste trimestre foi a Itália, mas essa não é a estréia dos italianos entre os 10 principais países.

Os Estados Unidos, sozinhos, produziram um total estimado de 2,1 milhões de novos zumbis neste trimestre, um aumento de 33% em relação ao período anterior. A Coréia do Sul apresentou o maior salto (de 45%) na criação de zumbis de um trimestre para outro, tendo contribuído com mais de meio milhão de novos zumbis neste trimestre. A Itália também praticamente dobrou sua produção de zumbis neste trimestre. Mesmo com o aumento global, dois países que contribuem pesadamente para a criação de zumbis, a China e a Rússia, tiveram ambos uma redução no número de novos zumbis criados.

T2 2009	
País	**%**
Estados Unidos	15,7
China	9,3
Brasil	8,2
Rússia	5,6
Alemanha	5,3
Itália	4,0
Rep. da Coréia	3,8
Índia	3,2
Reino Unido	3,0
Espanha	2,6
Total	**60,7**

Figura 3: 10 principais países com computadores zumbis recém-criados, por trimestre. Esses sistemas são sequestrados para enviar spam para milhões de endereços de e-mail.

Spam por país

O percentual total de spam produzido nos 10 principais países caiu 5% em relação ao último trimestre, indicando que mais países estão participando da produção de spam. Apesar disso, 65% da produção de spam ainda vem dessas 10 nações, as quais continuam a dominar o negócio.

Os remetentes de spam nos Estados Unidos podem estar sentindo os efeitos da crise econômica. Lá, a produção de spam caiu para 25% em comparação com os 35% do último trimestre. No entanto, os volumes de spam aumentaram em quase 80% desde o último trimestre, portanto, o volume estimado de spam oriundo dos Estados Unidos subiu quase 25%.

Brasil, Turquia e Polônia tiveram aumentos significativos, bem como aumentos consideráveis no volume total.

A Espanha volta aos 10 principais países após uma ausência de um trimestre e a República Tcheca faz sua estréia nesse grupo infame.

T2 2009		T1 2009		T4 2008	
País	**Porcentagem do total**	**País**	**Porcentagem do total**	**País**	**Porcentagem do total**
Estados Unidos	25,5	Estados Unidos	35,0	Estados Unidos	34,3
Brasil	9,8	Brasil	7,3	Brasil	6,5
Turquia	5,8	Índia	6,9	China	4,8
Índia	5,6	Rep. da Coréia	4,7	Índia	4,2
Polônia	4,9	China	3,6	Rússia	4,2
Rep. da Coréia	4,6	Rússia	3,4	Turquia	3,8
Rússia	2,4	Turquia	3,2	Rep. da Coréia	3,7
Romênia	2,3	Tailândia	2,1	Espanha	2,4
Espanha	2,1	Romênia	2,0	Reino Unido	2,3
Rep. Tcheca	1,9	Polônia	1,8	Colômbia	2,0
Porcentagem do total de spam global	**64,9**		**70,0**		**68,3**

Figura 4: Aproximadamente 65% do spam global tem origem em apenas dez países.

Spam por assunto

O seu farmacêutico deve estar fazendo hora extra com o aumento desenfreado da quantidade de spam de remédios que só podem ser vendidos com receita médica neste trimestre, representando 60% do total de spam que nossos sensores coletaram.

T2 2009		T1 2009		T4 2008		T3 2008	
Tipo de propaganda	**Porcentagem do total**	**Tipo de propaganda**	**Porcentagem do total**	**Tipo de propaganda**	**Porcentagem do total**	**Tipo de propaganda**	**Porcentagem do total**
Venda de remédios que exigem receita médica	60,0	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	16,0	Anúncios	21,9	Anúncios	19,3	Anúncios	19,3
Melhoria do desempenho sexual masculino	7,3	Réplicas de produtos	18,8	Melhoria do desempenho sexual masculino	16,8	Venda de remédios que exigem receita médica	10,7
DSN	6,6	Melhoria do desempenho sexual masculino	17,5	DSN	9,5	Storm	8,0
Réplicas de produtos	2,0	DSN	7,1	Encontros	3,9	DSN	7,7
Encontros	1,2	Storm	1,6	Réplicas de produtos	2,6	Últimas notícias	6,7
Storm	1,1	Diplomas	1,1	Empregos	1,7	Réplicas de produtos	6,0
Empregos	1,0	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	1,0	Empréstimos para quitação de dívidas	1,2	Operações bancárias	1,1
Outros	3,8	Outros	4,9	Outros	6,5	Outros	7,7
	100,0		**100,0**		**100,0**		**100,0**

Figura 5: Spam por tipo. O sempre popular spam de remédios que exigem receita médica mais que dobrou neste trimestre, saltando para 60% de todo o spam avaliado.

Figura 6: Essa "farmácia" envia a maior parte do spam atualmente.

A maior parte do spam que vemos hoje vem, supostamente, de uma única farmácia canadense. Esse site está geralmente vinculado a um URL chinês ou russo registrado com um registrador chinês. Uma característica singular desse spam é que ele alega ter sido enviado por solicitação do destinatário ou de um amigo deste, normalmente a partir de uma lista de discussão ou revista eletrônica. Esse tipo de spam, com todos os seus derivados, representa atualmente 60% do spam comum que vemos por aí. Embora existam muitas outras campanhas de spam, as de remédios que exigem receita médica são as que causam mais problemas se você não tiver filtros de spam apropriados.

Os ataques da Web mudam de alvo

No trimestre passado vimos várias manchetes relacionadas a explorações (exploits) de navegador, principalmente devido ao worm Conficker. Porém, neste trimestre, a atenção parece ter se voltado para os ataques a sites. Essa transição pode ser vista na figura 7, abaixo, que ilustra o número de novas páginas da Web explorando navegadores que são descobertas a cada dia. Houve vários ataques que atingiram sites legítimos durante o trimestre, muitos dos quais obtendo acesso utilizando roubo de senhas e injeção de SQL padrão. Os atacantes tipicamente inseriam scripts ocultos que redirecionavam os usuários para um domínio malicioso ou um conjunto de domínios maliciosos, os quais tentavam induzir o usuário a instalar sua carga útil ou encontravam uma vulnerabilidade não corrigida no conjunto de ferramentas de navegação na Web do usuário.

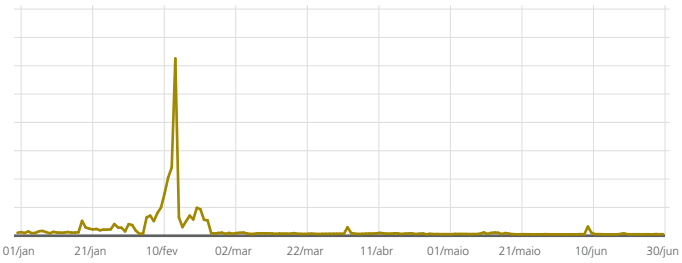


Figura 7: Páginas da Web descobertas diariamente que exploram navegadores.

Entre os ataques que chamaram a atenção da mídia estava o Gumblar, que apareceu pela primeira vez no final de abril, com um pico por volta do final de maio. Seguiram-se os ataques Martuz e Beladen. Lemos manchetes alardeando milhares de sites legítimos infectados. Independente do número real, esses ataques apenas redirecionam os usuários para os principais sites servidores de malware que já vimos. É interessante que, muito depois desses domínios maliciosos serem desativados, eles continuaram recordistas de resultados de pesquisa no Google.[4] Essa longevidade demonstra quanto tempo é necessário para muitos servidores Web legítimos perceberem que foram atacados e reparar os danos.

O Gumblar também ilustra a frequência com que esses sites, servidores e URLs maliciosos são reutilizados para várias atividades. Ao monitorar e rastrear o Gumblar, identificamos vários domínios que operavam em conjunto com essa exploração (exploit). 71% dos domínios que identificamos nesse ataque já tinham sido observados e utilizados em outros ataques. Mais 13% dos domínios já tinham sido "merecedores" de nossa designação TrustedSource Malicious Web Reputation (reputação maliciosa na Web) antes de participarem do ataque atual. (O rótulo TrustedSource Malicious Web Reputation baseia-se em análises comportamentais avançadas que identificam o site como potencialmente nocivo.)

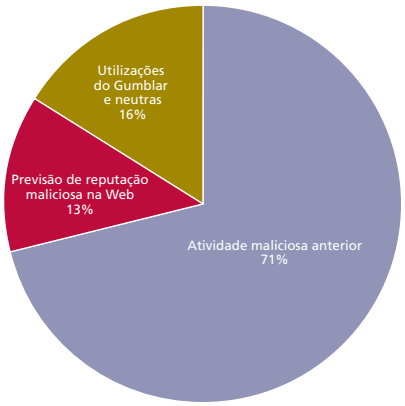


Figura 8: Sites do Gumblar, por tipo.

4 Google Online Security Blog, "Top 10 Malware Sites" (10 principais sites de malware). http://googleonlinesecurity.blogspot.com/2009/06/top-10-malware-sites.html

Como está o cenário de ameaças da Web como um todo neste trimestre? Ignorando o efeito do Conficker em abril, que chamou uma atenção considerável da mídia, vimos uma leve diminuição na taxa de crescimento de URLs com reputação maliciosa na Web em comparação com o último trimestre. Um dos motivos dessa diminuição está relacionado à evolução dos domínios maliciosos. Historicamente, nós identificamos e protegemos contra muitos desses domínios assim que eles se registram. Isso continua valendo quase sempre, embora agora estejamos vendo novas tendências nos métodos que os domínios maliciosos utilizam para se registrar e os sites com os quais esses domínios se associam. Como os cibercriminosos parecem se ajustar às técnicas de segurança para rastreamento e avaliação dos serviços de hospedagem e os tipos de atividades que estes suportam, os atacantes estão adotando novas maneiras de se esconder. Isso causou uma diminuição no número de domínios que podemos identificar como maliciosos quando do registro. No entanto, os picos observados durante este trimestre correlacionam-se com domínios maliciosos observáveis utilizando práticas de registro de domínio e outros indicadores preditivos, portanto, nossos métodos tradicionais de associação ainda são bastante eficazes.

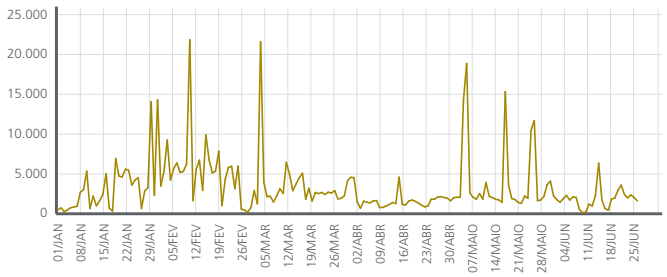


Figura 9: Novos sites com reputações maliciosas, informados diariamente

Não vimos alterações significativas no que se refere à localização dos servidores Web maliciosos. (Veja a figura 10, abaixo.) No entanto, quando deixamos de considerar servidores individuais e nos concentramos nos domínios e URLs hospedados nesses servidores, a perspectiva geográfica muda. (Veja a figura 11, abaixo.) Isso traz à luz alguns novos países que compõem a lista — incluindo Austrália e Bahamas. Esta última tem uma média de 1.482 URLs maliciosos por servidor Web malicioso. Neste trimestre, nossas investigações de servidores maliciosos na América Central e no Caribe aumentaram.

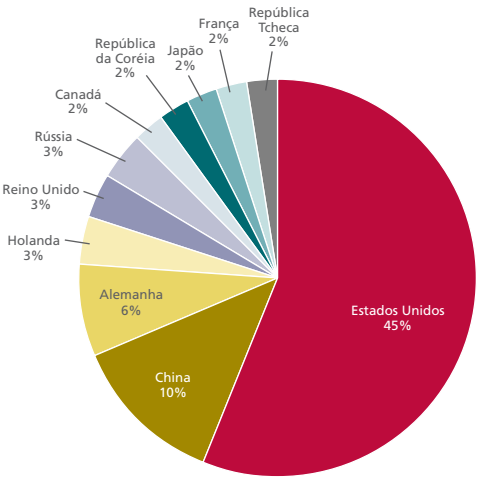


Figura 10: Distribuição de servidores Web com reputações maliciosas.

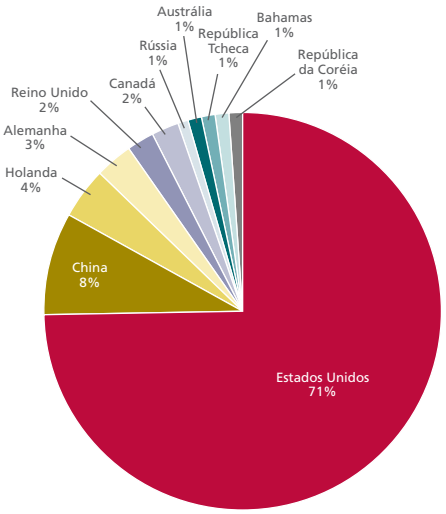


Figura 11: Distribuição do total de URLs com reputações maliciosas

Vindo de um lar próximo ao seu

Uma outra ameaça da Web vem de máquinas domiciliares desprotegidas. Esses sistemas podem estar infectados e controlados por pessoas de fora, como parte de suas "redes de bots de aluguel", e podem estar sendo utilizados para enviar spam, roubar informações dos usuários domésticos e muito mais. Também vimos usuários domésticos configurando vários serviços de acesso remoto, anonimizadores e serviços similares para ter acesso a seus computadores domiciliares de qualquer lugar — incluindo a rede corporativa. Neste trimestre examinamos quais sites residem nesses sistemas. Nós excluímos todos os PCs domiciliares que *não* estavam hospedando sites ativos e anunciados. Dos que estavam hospedando sites ativos, não foi uma surpresa constatar que a maioria estava servindo URLs de spam.

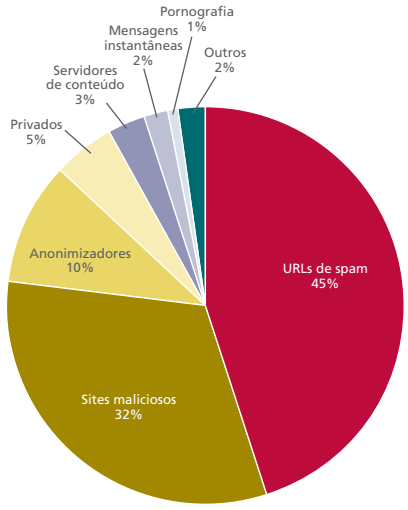


Figura 12: Sites sediados em domicílios, por utilização

Malware e programas potencialmente indesejados

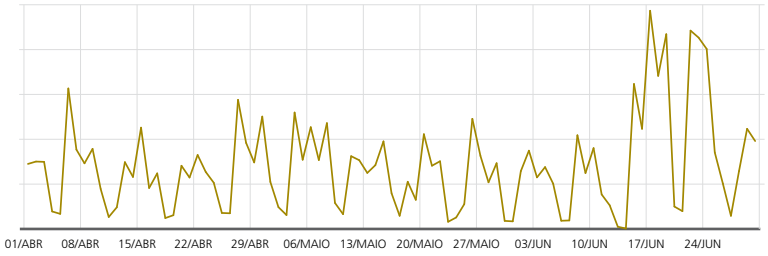


Figura 13: Novos sites que fornecem malware e programas potencialmente indesejados, por dia

Fora a comoção causada pelo Conficker, este trimestre foi um pouco mais tranquilo que o anterior no que se refere a sites rotulados como Malicious Web Reputation (reputação maliciosa na Web). No entanto, o trimestre está terminando com força. Nas últimas semanas, houve uma atividade significativa em injeções de SQL e iframe, otimização de mecanismos de pesquisa, downloaders, spoofers, falsos programas antivírus e mais. Por exemplo, após a morte de Michael Jackson, vimos um aumento tanto de spam quanto de malware relacionados às notícias. Os atacantes imediatamente trabalharam com mecanismos de pesquisa para tentar redirecionar os usuários para um site antivírus falso ou um vídeo em Flash infectado. Além disso, vimos esses servidores aumentarem a diversidade de seus ataques em sua busca por um que seja bem-sucedido em infectar os visitantes.

Examinando os tipos de malware e programas potencialmente indesejados (PUPs) transferidos por download dos servidores Web, descobrimos que houve pouca mudança nos tipos predominantes entre este trimestre e o anterior. Os PUPs genéricos são maioria entre os downloads via Web.

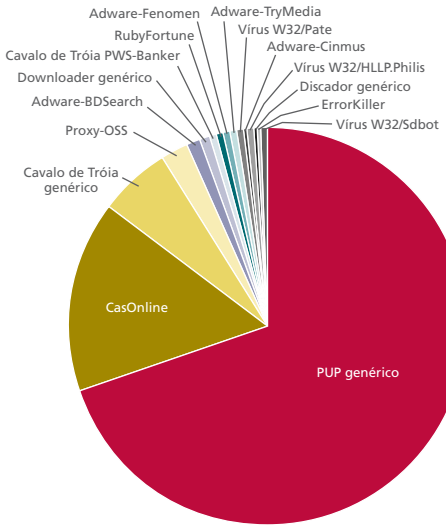


Figura 14: Predomínio de downloads de malware e PUPs, por tipo

Web 2.0 e Twitter

Com os eventos deste trimestre — o acidente da Air France, eleições iranianas, as mortes de Farrah Fawcett e Michael Jackson — o mundo revelou já estar pronto para a Web 2.0. A pergunta é se a Web 2.0 está totalmente pronta para o mundo. Tanto o Facebook quanto o Twitter tiveram surtos de atividade com o anúncio da morte do Rei do Pop. Em primeiro lugar, essa atividade ultrapassou os riscos de segurança associados ao evento da notícia. Conforme o mundo avança para essa nova forma de comunicação, os phishers e autores de malware seguem ativamente o mesmo caminho.

Existem alguns riscos de segurança característicos desses sites de rede social. Muitos dos riscos estão relacionados ao grande número de recursos e aplicativos que tantas pessoas executam sem pensar duas vezes. Essa atitude displicente permitiu que vários worms, ataques de phishing e outras atividades maliciosas entrassem em ação. Por exemplo, existem muitas ferramentas de rede social que fazem toda sorte de coisas para os usuários — desde monitorar contas bancárias até bloquear e ocultar de outras pessoas. A chave é que muitas dessas "ferramentas" exigem que os usuários digitem nomes de usuário e senhas. Infelizmente, muitas pessoas sentem-se tão à vontade com a interatividade da Web 2.0 que se esquecem das noções básicas de segurança on-line. Uma vez que atacantes tenham acesso a credenciais de contas, eles passam a ter pleno acesso aos amigos das vítimas e podem perpetrar todo tipo de ataque. Esse fenômeno dá um novo significado à expressão "fogo amigo".

Desde sua criação em 2006, o Twitter ganhou enorme popularidade no mundo todo. É um dos aplicativos mais frequentemente utilizados na Internet atualmente, estando em 27° lugar (na avaliação do Alexa) em volume de tráfego de Internet. Era só uma questão de tempo para que malware, phishing e fraudes começassem a ocorrer — utilizando ou visando o Twitter e seus usuários. Além disso, o Twitter tornou-se lugar-comum tanto em empresas quanto entre consumidores. Essa exposição deu aos atacantes um meio de direcionar os seguidores para vários URLs. Devido ao espaço limitado associado ao "tweeting", muitos métodos, especialmente o TinyURL, são amplamente populares para maximização do espaço. (TinyURL é um serviço Web que substitui um URL longo por um atalho curto que redireciona os navegadores para o endereço completo.) Embora o TinyURL seja um serviço útil, os usuários não têm como saber para onde estão sendo redirecionados antes de tentar acessar a página. Portanto, o cuidado que os usuários normalmente têm quando visualizam resultados de pesquisa e links de notícias desaparece por trás do endereço alternativo, restando apenas a segurança de suas máquinas desktop e gateway para protegê-los.

Em abril, a plataforma de microblog enfrentou vários ataques de worms em JavaScript explorando uma vulnerabilidade de script entre sites (XSS) para infectar outros perfis de usuário. O primeiro alerta ocorreu quando os perfis do Twitter começaram a postar mensagens incentivando as pessoas a visitar o StalkDaily.com, um concorrente do Twitter. Mikeyy Mooney, de 17 anos, criador desse clone de Twitter, assumiu a responsabilidade: "Eu sou a pessoa que escreveu o código do XSS que atuava como worm ao atualizar automaticamente o perfil e o status dos usuários e que infectava outros usuários que visualizavam seus perfis. Para ser sincero, fiz isso por tédio. Eu normalmente gosto de descobrir vulnerabilidades dentro de sites e tento não causar muito dano, mas inicio um worm ou alguma coisa para dar aos desenvolvedores uma dica sobre o problema e, fazendo isso, promovo a mim mesmo e ao meu site."[5]

Horas mais tarde, depois que o Twitter afirmou ter resolvido o problema, um novo worm semelhante entrou na comunidade. Novamente, quando um perfil infectado era visualizado, ele era executado e injetava um código no perfil do visualizador que passava adiante a infecção. Dois outros ataques ocorreram no dia seguinte, forçando a equipe do Twitter a excluir quase 10.000 tweets que estavam espalhando o worm.

Alguns dias depois, Travis Rowland, fundador e CEO da exqSoft Solutions, uma empresa de desenvolvimento de aplicativos Web personalizados, confirmou ter oferecido a Mooney um emprego na empresa e que ele aceitou. Essa notícia é surpreendente e lamentável, pois criar código malicioso não deveria contribuir para a obtenção de um emprego, nem como credenciais positivas para contratação.

Enquanto isso, surgiram novas variantes com referências a celebridades.

5 BNOnews, "17-year-old claims responsibility for Twitter worm" (Jovem de 17 anos assume responsabilidade por worm do Twitter). http://www.bnonews.com/news/242.html

Hackers no Twitter

Pela segunda vez este ano, um hacker alega ter obtido acesso administrativo à conta de um funcionário do Twitter.[6]

Em abril, um hacker francês anônimo chamado Hacker Croll postou capturas de tela em um fórum de discussão on-line francês. As imagens foram aparentemente capturadas enquanto o hacker estava conectado à conta Twitter de Jason Goldman, um diretor de gerenciamento de produto da Twitter.

Figura 15: Até o Twitter sofreu com hackers obtendo acesso a contas de administradores.

Ferramentas de marketing ou de spam?

Se você duvida do poder que o Twitter proporciona, seja no presente ou no futuro, basta procurar algumas ofertas que aparecem na Internet.

6 Twitter, "Unauthorized Access: An Update on Security" (Acesso não autorizado: uma atualização sobre segurança). http://blog.twitter.com/2009/04/unauthorized-access-update-on-security.html

Figuras 16a, 16b e 16c: O Twitter está cheio de oportunidades para vendas, mas elas são marketing ou spam? Muitos desses serviços exigem que os usuários divulguem informações de login — o que nunca é uma boa idéia.

Spam de Twitter

Sem dúvida encontraremos spam depois da morte. Ele já chegou ao Twitter.

Figuras 17a e 17b: O spam de Twitter fornece mensagens familiares, como demonstram estes exemplos.

Twitter, um alvo para a pesquisa de vulnerabilidades

Já se passou algum tempo desde o "Month of Apple Bugs" (mês dos bugs da Apple) ou o "Month of PHP bugs" (mês dos bugs de PHP), portanto, já é hora do "Month of Twitter Bugs" (mês dos bugs do Twitter), programado para julho deste ano. Estamos aguardando as inevitáveis falhas de script entre sites (XSS) e solicitações entre sites forjadas (CSRF) que colocam os usuários do Twitter em risco de ataques de hackers maliciosos.

Raff Aviv, que está por trás do projeto, escreveu em seu site: "Todo dia eu publico uma nova vulnerabilidade em um serviço de terceiros para o Twitter no site twitpwn.com. Como essas vulnerabilidades podem ser exploradas para criar um worm de Twitter, vou dar ao provedor de serviços e ao Twitter pelo menos 24 horas de vantagem antes de publicar a vulnerabilidade."[7]

Estamos satisfeitos de ver o Twitter receber um pequeno empurrão para resolver brechas potenciais e reduzir o risco para sua grande base de usuários, embora uma notificação com apenas 24 horas de antecedência não nos pareça uma atitude responsável. A história mostra que sites de alto tráfego que fazem uso pesado de tecnologias Web 2.0 serão explorados se não forem corrigidos.

A volta do hacktivismo

Neste trimestre, o Twitter desempenhou um papel nos desdobramentos da eleição iraniana. Os usuários do Twitter transmitiram informações sobre protestos contra o governo. O Twitter também foi o canal para distribuição de ferramentas de ataque de negação de serviço e para a coordenação desses ataques contra vários sites de notícias iranianos.

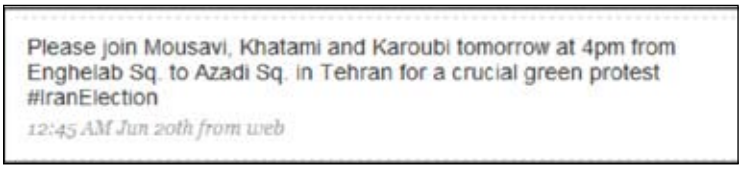


Figura 18: Os iranianos usaram o Twitter para protestar contra o regime.

Independente das tendências políticas de cada um, o uso do Twitter para disseminar informação e para coordenar ação mostra o poder das ferramentas de rede social em geral e do Twitter, especificamente.

Figura 19: O Twitter e outras ferramentas de rede social são uma força poderosa.

O Twitter pode ser a atual menina dos olhos das redes sociais, mas ele não está sozinho. O Facebook continua sendo um serviço popular, tanto entre usuários quanto criadores de malware. O Avert Labs continua a ver um aumento no principal malware, o Koobface, que atinge usuários do Facebook. (Veja a figura 20, abaixo.) Esse malware ainda é uma das ameaças mais predominantes que rastreamos.

7 Aviv Raff On .NET. http://aviv.raffon.net/2009/06/15/MonthOfTwitterBugs.aspx

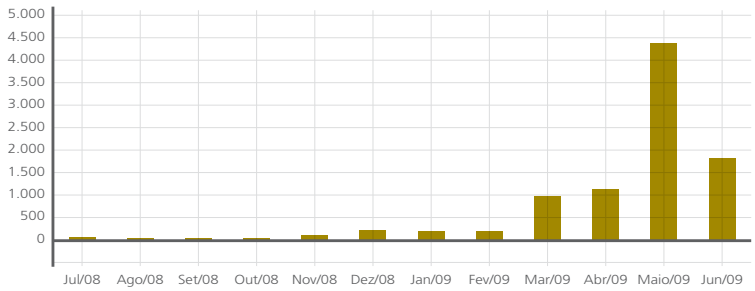


Figura 20: Binários de Koobface exclusivos descobertos, por mês. O mês de maio teve um salto enorme em ameaças.

Phishing

Neste trimestre vimos um aumento no número de URLs de phishing visando bancos estrangeiros e em idiomas estrangeiros. Também vimos uma criação em massa de sites utilizando diversos kits e metodologias, sendo esses kits multilíngues. Por exemplo, encontramos um kit utilizado para gerar 1.784 sites de phishing. A versão francesa desse kit foi utilizada para gerar 214 sites de phishing. Em 28 de maio, houve um grande pico em novos URLs de phishing. Muitos destes espalharam-se além de fronteiras e utilizaram vários kits.

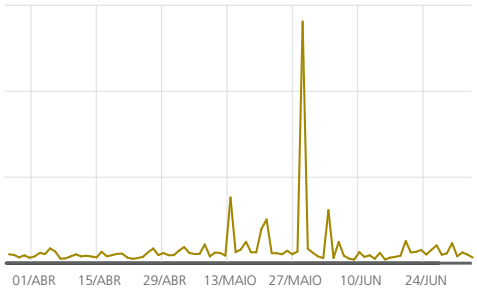


Figura 21: Novos sites de phishing descobertos, por dia. Em 28 de maio, os phishers excederam em muito seu empenho habitual.

Os Estados Unidos continuam a hospedar mais sites de phishing do que qualquer outro país. Determinadas nações hospedam sites mais "arriscados". Essa seleção costuma ser a mesma sempre que avaliamos.

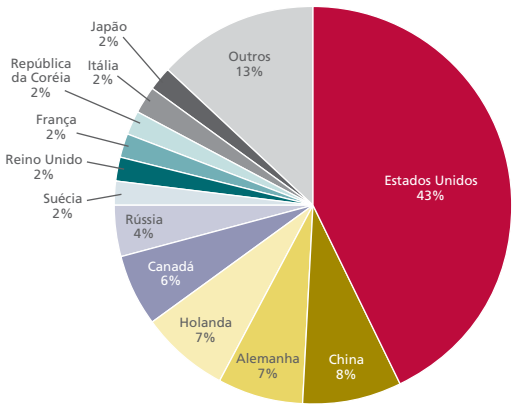


Figura 22: Distribuição dos sites de phishing.

Malware: a face do cibercrime

Em muitos aspectos, o cibercrime evoluiu paralelamente aos computadores e à maneira como as pessoas os utilizam. Desde os estágios preliminares, tanto da informática quanto da Internet, houve malware e cibercrime, embora ainda não utilizássemos esses termos. Os vírus atacavam o setor de boot, eram parasitas e eram distribuídos principalmente através de disquetes. As fraudes e o spam também apareceram bem cedo e tinham o mesmo objetivo que hoje em dia — roubar alguma coisa. Com a ampla utilização da Internet, o malware e o cibercrime evoluíram para acompanhar as mudanças no comportamento dos usuários. As vidas de muitas pessoas agora estão completamente vinculadas ao uso do computador. Seja ao pagar contas on-line, nos blogs ou na interação com outros usuários do Facebook e do Twitter, as pessoas e seus dados de identidade agora são digitais. Os cibercriminosos e autores de malware compreendem perfeitamente essa dinâmica e sempre acompanharam essa evolução, a qual já era esperada por alguns. Seu atual conjunto de ferramentas e serviços reflete essa compreensão, com o cibercrime tornando-se cada vez mais um negócio de serviços.

Cavalos de Tróia para roubo de senhas crescem rapidamente

Os cavalos de Tróia que roubam senhas continuam a ser uma das ferramentas favoritas dos cibercriminosos. As ferramentas para criar esses cavalos de Tróia estão amplamente disponíveis na Internet e há muitos sites dedicados à sua venda como um serviço. Sua função é simples: Eles roubam senhas. É a complexidade do próprio cavalo de Tróia que o torna tão bem-sucedido.

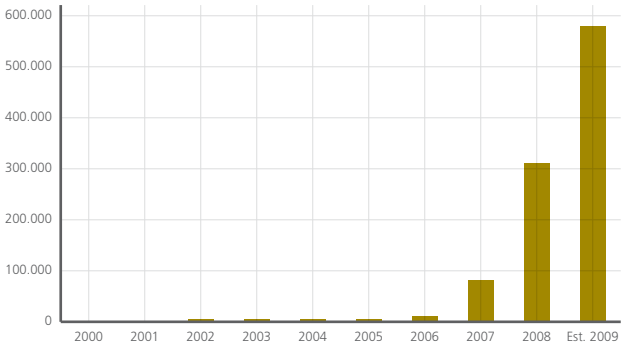


Figura 23: Crescimento no malware para roubo de senhas

Os cavalos de Tróia para roubo de senhas frequentemente infectam usuários que abrem anexos de e-mail que fazem download de malware de sites maliciosos. Uma vez instalados, os cavalos de Tróia coletam nomes de usuário e senhas de uma grande variedade de programas, como Internet Explorer, sessões de FTP e vários jogos on-line, incluindo o *World of Warcraft*. Os dados de identidade coletados são enviados para um servidor administrado por cibercriminosos, os quais os vendem de várias maneiras — incluindo sites de leilão ou no atacado — para um comprador.

O Avert Labs observou uma complexidade crescente nesses programas maliciosos. Eles estão mais furtivos do que nunca e costumam ter mecanismos de autoproteção para assegurar sua sobrevivência em um PC comprometido. Eles também estão se tornando mais genéricos por natureza. Nos anos anteriores, os cavalos de Tróia eram específicos para a instituição visada. Ultimamente, porém, eles vêm coletando cada vez mais dados de uma variedade maior de alvos, maximizando sua eficácia. Por que visar só um banco ou jogo quando se pode coletar dados de todos?

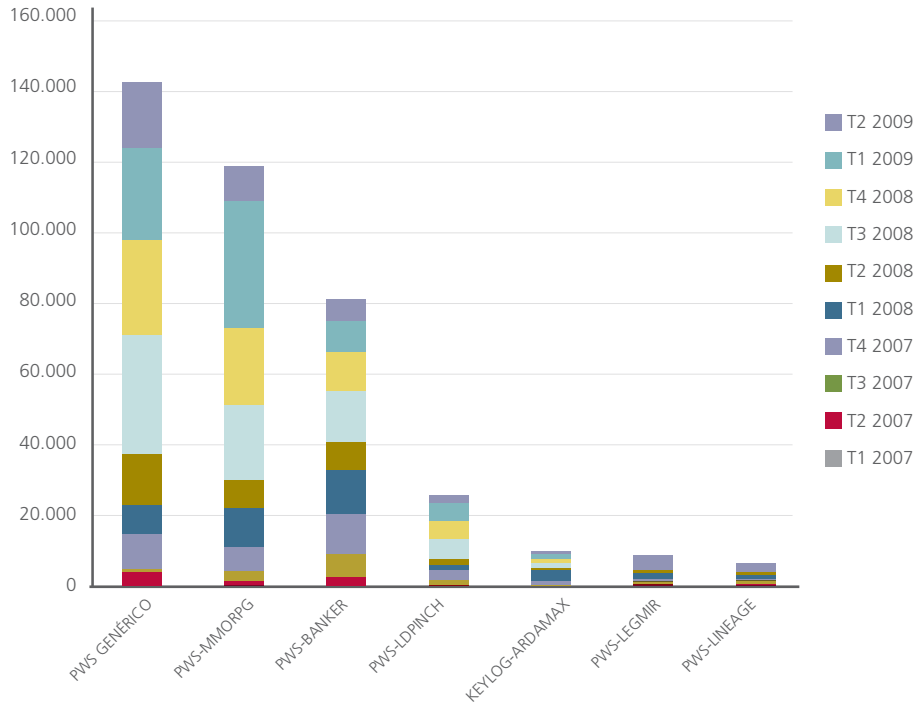


Figura 24: Principais variantes para roubo de senhas, por nome e trimestre

Zeus

Esse deus deve estar irado. Zeus (também conhecido como Zbot e WSNPoem) é um aplicativo construtor para criação de cavalos de Tróia para roubo de senhas. Ele inclui um painel de controle feito na linguagem de script de Web PHP e um executável de Windows para construir o malware. O arquivo produzido pode roubar dados e credenciais, capturar tráfego de HTTP e HTTPS, capturar telas, enviar seus registros para um local remoto e atuar como servidor proxy. Os registros, que são codificados, podem ser descriptografados pelo construtor. Os usuários do Zeus podem encontrar várias opções, como pacotes de exploração (exploit) e uma avançada interface de comando e controle.

O Zeus teve um trimestre agitado:

- A versão 1.2.4.x foi colocada à venda em abril.
- Seus autores russos aumentaram seus serviços para iniciantes. (Veja a figura 25.)

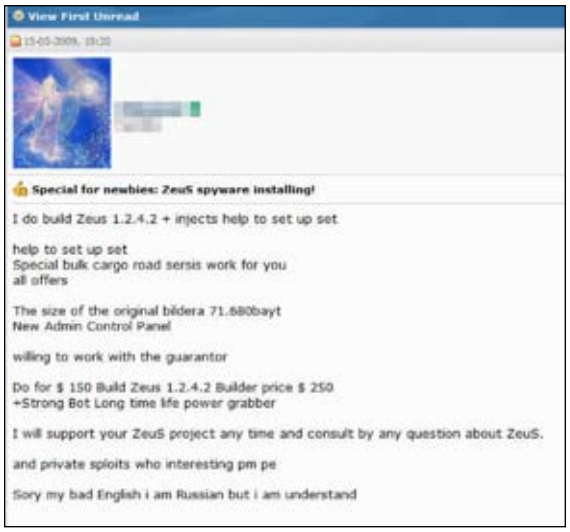


Figura 25: Os autores do Zeus oferecem incentivos a mais.

- Roman Hüssy é um especialista em TI suíço de 21 anos que administra o Zeustracker, um site que lista os servidores de Internet que utilizam o Zeus.[8] Hüssy observou o "suicídio" inesperado de 100.000 sistemas infectados localizados principalmente na Polônia e na Espanha. Um "botmaster" utilizou a rotina "matar sistema operacional" para derrubar as conexões de Internet das máquinas infectadas. Guerra entre rivais ou ação voluntária para eliminar alguns vestígios? Ambas as possibilidades são plausíveis.[9]

Figura 26: Registros "novinhos" de Zeus à venda.

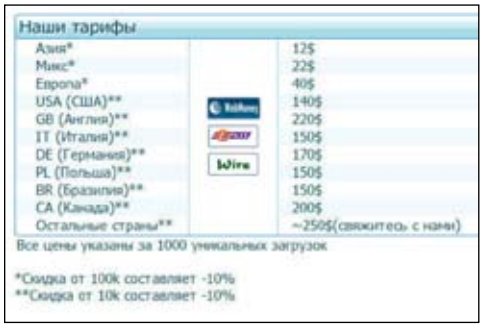
- ZeuEsta está de volta on-line. Os assinantes desse serviço recebem um iframe específico que eles podem adicionar a sites-armadilha que eles conheçam ou que tenham comprometido. O iframe redireciona suas vítimas para uma página do ZeuEsta para infectá-las com malware. Os assinantes também obtêm acesso protegido por senha a um painel de administração pessoal para visualizar registros, bots on-line, estatísticas de exploração, para emitir comandos, etc. Liberty Reserve hospeda ZeuEsta por US$ 100 por mês.

8 https://zeustracker.abuse.ch/monitor.php?filter=online
9 Security Fix (Correção de segurança), The Washington Post. http://voices.washingtonpost.com/securityfix/2009/05/zeustracker_and_the_nuclear_op.html

Figura 27: O serviço ZeuEsta torna fácil para os cibercriminosos entrar no negócio.

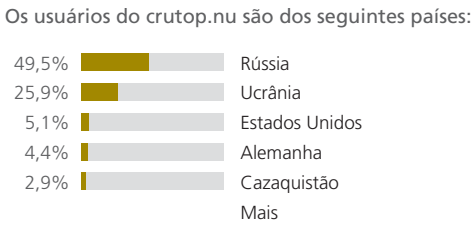
Crimeware como serviço

O caso Zeus demonstra a evolução para um modelo de mais serviços no cibercrime. "Se você tem o malware, eles têm os computadores vulneráveis!" Alguns cibercriminosos instalam malware criado por outras pessoas em máquinas comprometidas que eles controlam.



Figuras 28a e 28b: Seu malware instalado em 1.000 computadores por apenas US$ 140.

A comissão federal de comércio (FTC) dos EUA teve êxito em deter mais um cibercriminoso. O falso provedor de serviços de Internet Pricewert LLC, utilizando vários nomes, como 3FN.net, Triple Fiber Network e APS Communications, foi fechado pela FTC. De acordo com os agentes federais, essa empresa recrutava, hospedava conscientemente e participava ativamente na distribuição de spam, pornografia infantil e outros tipos de conteúdo eletrônico nocivo. Pesquisando o site da divisão corporativa da secretaria do estado de Oregon (EUA), descobrimos que a Pricewert foi registrada em Portland em setembro de 2003, com duas empresas de Belize constando como membros. Em seu memorando, a FTC relaciona o conteúdo ilegal hospedado pelo 3FN: software malicioso de rede de bots, pornografia infantil, produtos antivírus falsos, farmácias on-line ilegais e pirataria de software e músicas.[10] A FTC explica como a equipe da 3FN utilizou o fórum crutop.nu para recrutar novos clientes. Consultas ao Alexa.com mostram que russos e ucranianos são os principais visitantes desses sites.



Figuras 29a e 29b: A FTC fechou um falso provedor de serviços de Internet cujas atividades ilegais atraíam, principalmente, o interesse da Rússia e da Ucrânia.

10 Corte Distrital dos Estados Unidos, Distrito do Norte da Califórnia, "Memorandum of Points and Authorities in Support of Plaintiff's Motion for an *ex parte* Temporary Restraining Order and Order to Show Cause" (Memorando de pontos e autoridades em apoio à moção de Plaintiff por uma ordem para demonstração de causa e ordem cautelar provisória "ex parte"). http://www.ftc.gov/os/caselist/0923148/0906043fnmemotro.pdf

Malware de AutoRun

O malware com base em memória Flash e USB (também chamado de malware de AutoRun) continua a ser uma das famílias mais predominantes dentre todo o malware identificado pelo Avert Labs diariamente. Os usuários adoram seus convenientes dispositivos e os criadores de malware adoram os dados dos usuários. Quando levamos em consideração os tipos de dispositivos que o malware de AutoRun pode infectar — "pen drives", porta-retratos digitais e dispositivos de armazenamento maiores — o perigo para os dados, tanto do consumidor quanto corporativos, não pode ser menosprezado. Para saber mais sobre infecções por AutoRun e como combatê-las, leia nosso relatório *A ascensão do malware com base em AutoRun*, de autoria de pesquisadores do Avert Labs em nossos escritórios de Bangalore, na Índia.[11]

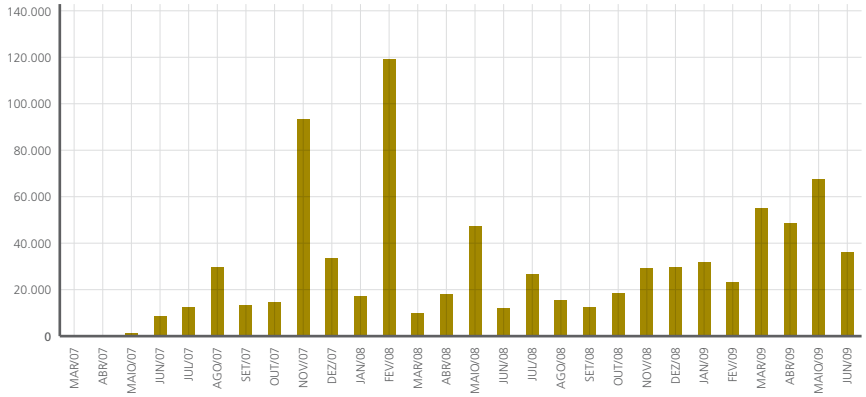


Figura 30: Binários de malware de AutoRun exclusivos descobertos, por mês.

Na figura 30 podemos ver que em alguns meses houve grandes saltos nas versões do malware de AutoRun. Apesar dos altos e baixos, a tendência geral é de alta. A funcionalidade do AutoRun é significativamente conveniente para os criadores de malware. (Ela economiza um par de cliques.) Esse recurso do Windows conseguiu, sozinho, dar vida nova ao modelo de propagação de malware "de bolso" dos anos 80. Famílias de cavalos de Tróia predominantes, como PWS-OnlineGames e PWS-Gamania, que antes exigiam que o usuário clicasse em um executável, agora usam o vetor AutoRun para se disseminar através de unidades removíveis. Famílias de vírus parasitas, como W32/Sality e W32/Virut, também incorporaram esse vetor de infecção com um certo grau de êxito.

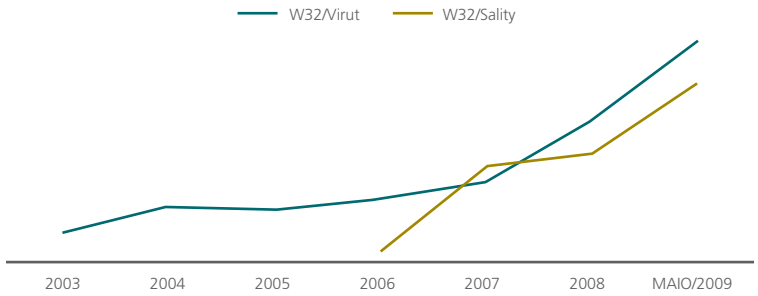


Figura 31: Crescimento dos vírus parasitas de USB W32/Sality e W32/Virut.

Continuamos a observar um aumento alarmante no malware que utiliza o AutoRun como vetor de infecção. Veja a seguir um exemplo do quão desenfreado é o problema do malware de AutoRun: A figura 32, abaixo, mostra dados do mapa global de vírus da McAfee, que rastreia estatísticas de infecções observadas em computadores que executam software antivírus da McAfee.

11 http://www.mcafee.com/us/local_content/white_papers/wp_autorun_malware_v8_en.pdf

Figura 32: O mapa global de vírus da McAfee coloca o malware de AutoRun (aqui chamado Generic!atr) no topo da lista.

No trimestre passado, o worm Conficker atraiu muito interesse da imprensa. Contudo, sua importância empalideceu quando comparado com detecções de AutoRun, como informamos em nosso último número. Embora tenha havido um leve aumento na atividade do Conficker neste trimestre, isso não se compara ao predomínio do AutoRun.

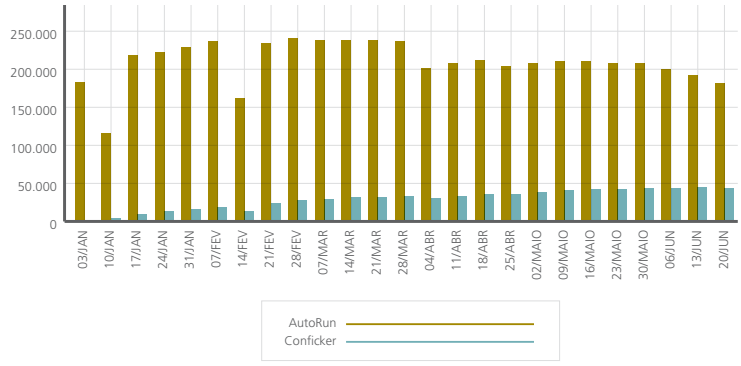
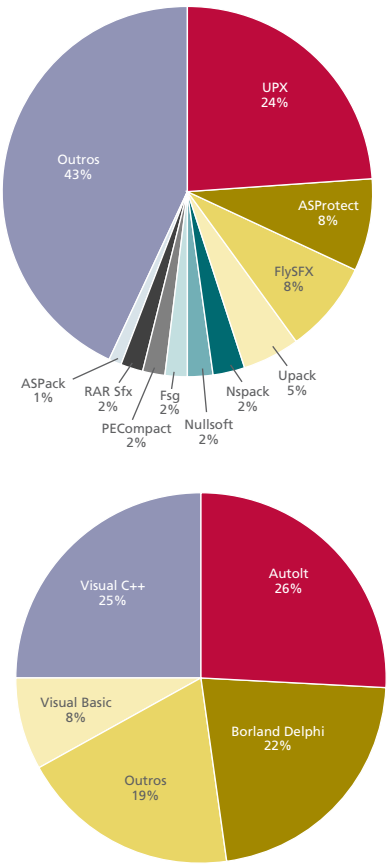


Figura 33: As infecções por AutoRun continuam a superar as do worm Conficker, apesar da grande cobertura de mídia deste último.

Descobrimos malware de AutoRun em mais de 27 milhões de arquivos infectados durante um período de 30 dias neste trimestre, o que o torna o elemento de malware número um detectado globalmente. Considerando-se os milhões de computadores na Internet e detecções de ameaças com base em AutoRun realizadas por fornecedores de segurança, compreende-se a gravidade do problema. Os compiladores e empacotadores utilizados para criar a maior parte dessa família de malware estão prontamente disponíveis, sendo, frequentemente, as mesmas ferramentas utilizadas pelos fabricantes de software legítimos.



Figuras 34a e 34b: O predomínio de empacotadores (em cima) e compiladores (embaixo) legítimos durante o trimestre torna fácil para os atacantes preparar worms do tipo AutoRun para distribuição.

Quais conclusões podemos tirar da popularidade do UPX e do AutoIt para criação de malware de AutoRun? A resposta rápida é que são programas gratuitos e de código aberto. O código-fonte para criação de worms com base no AutoIt, por exemplo, está amplamente disponível na Internet. Além disso, os arquivos compilados com as versões 3.2x e anteriores do AutoIt podem ser facilmente descompilados até o script original. Isso é muito conveniente para a criação de versões novas e atualizadas de malware.

A Microsoft resolveu muitos vetores de infecção predominantes no passado — como a disseminação através de setores de boot, macros do Office, scripts e clientes de e-mail — através de recursos de segurança aprimorados. Com a alta das infecções com base em AutoRun, a Microsoft poderia fazer uma grande diferença corrigindo essa conveniência tão explorada em futuras atualizações do Windows.

Sobre o McAfee Avert Labs

McAfee Avert Labs é o grupo 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. Respaldada por uma equipe de pesquisa ganhadora de vários prêmios, a McAfee cria produtos inovadores que proporcionam a usuários domésticos, empresas, setor público e provedores de serviços a capacidade de cumprir com regulamentos, proteger dados, evitar interrupções, identificar vulnerabilidades e monitorar e aprimorar continuamente sua segurança. 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

6623rpt_avert_threat_0709_ETMG