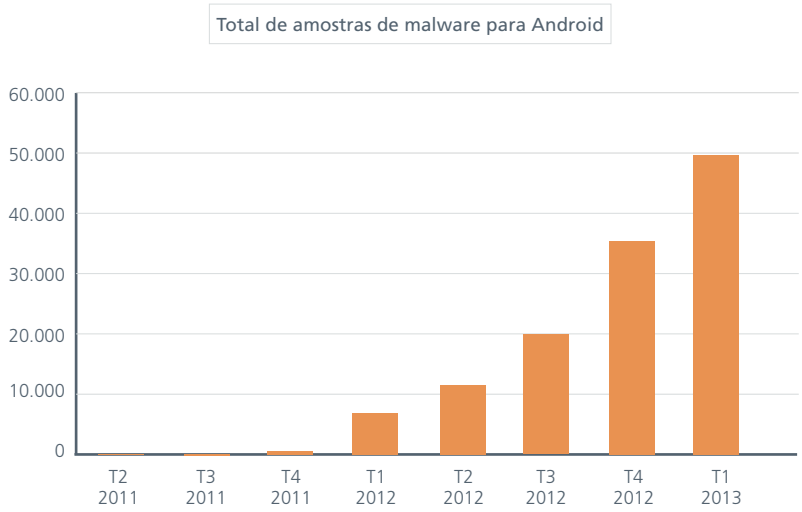
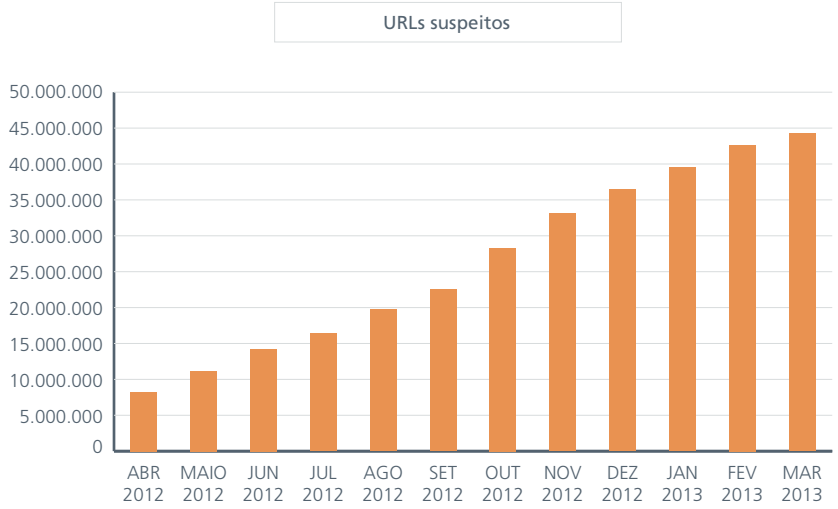
No primeiro trimestre de 2013, a comunidade cibercriminosa global adotou uma tática "De Volta para o Futuro" em sua busca incansável por vítimas e lucros. Muitas das tendências mais marcantes observadas pelo McAfee Labs nos três trimestres anteriores perderam o ímpeto, enquanto tipos de ataque mais antigos e que poderíamos chamar de "malware retrô" tiveram um novo crescimento significativo.

Exemplos de tendências marcantes de ameaças que arrefeceram no primeiro trimestre de 2013 são:

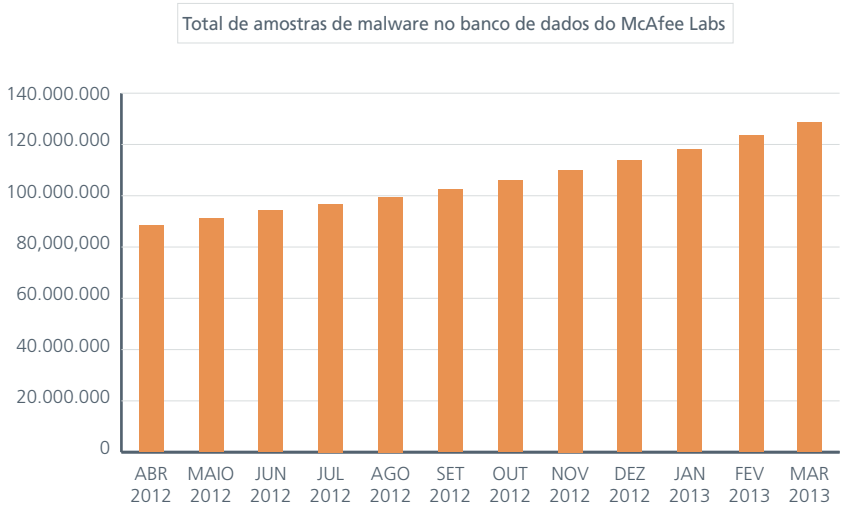
Desaceleração no surgimento de malware móvel (para Android) novo. Embora o número absoluto de novas amostras para Android tenha aumentado 40%, isso representou uma redução de 10% na taxa de crescimento, em comparação com o quarto trimestre de 2012.



Da mesma forma, o número de URLs maliciosos detectados na Web aumentou 12% no primeiro trimestre, mas a taxa de crescimento, que foi superior a 80% no quarto trimestre, caiu quase 40 pontos percentuais.



Até mesmo o crescimento nas amostras de malware conhecidas caiu um pouco no primeiro trimestre, para 28%, em comparação com os 38% do quarto trimestre de 2012. O McAfee Labs adicionou mais de 14 milhões de novas amostras de malware ao "zoológico" no primeiro trimestre.



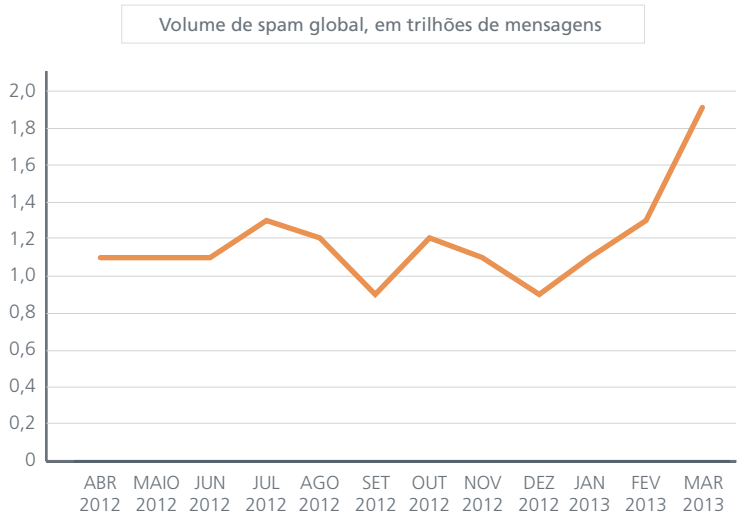
Finalmente, a taxa de crescimento no volume bruto de ladrões de senhas, ransomware, antivírus falsos e rootkits descobertos ficou relativamente estável no primeiro trimestre. Todas essas ameaças continuam a aumentar em números absolutos, embora suas taxas de crescimento tenham sofrido uma leve queda.

Contudo, essa desaceleração nas taxas de crescimento não significa que o ciberespaço está se tornando mais seguro. Pelo contrário; considerando-se outras tendências observadas no primeiro trimestre, pode-se afirmar que a comunidade cibercriminosa está ficando mais esperta e mais disciplinada ao demonstrar uma preferência por ataques direcionados voltados contra comunidades e localizações geográficas específicas. Como toda empresa, os grupos cibercriminosos querem otimizar sua eficiência e aumentar seus lucros. A tendência observada em relação a ataques direcionados parece indicar que o cenário global de ameaças está indo em uma direção nova e mais perigosa.

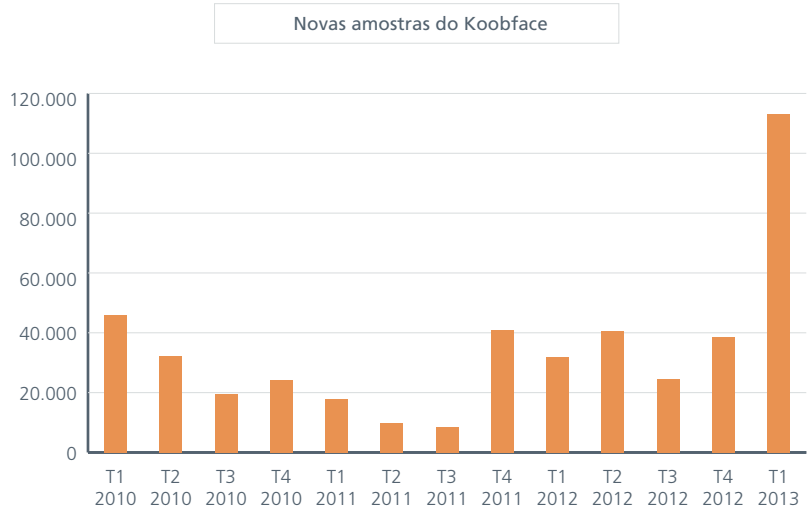
Um exemplo claro dessa tendência para ataques direcionados pode ser encontrado no cavalo de Troia Citadel. Originalmente desenvolvido para roubar dinheiro de bancos bem específicos, o Citadel foi aperfeiçoado e agora pode ser utilizado para extrair informações pessoais das vítimas visadas pelo atacante.

Outras tendências de ameaças no primeiro trimestre que remetem a tempos passados, mas que agora estão se evidenciando em ataques direcionados e mais perigosos, são as seguintes:

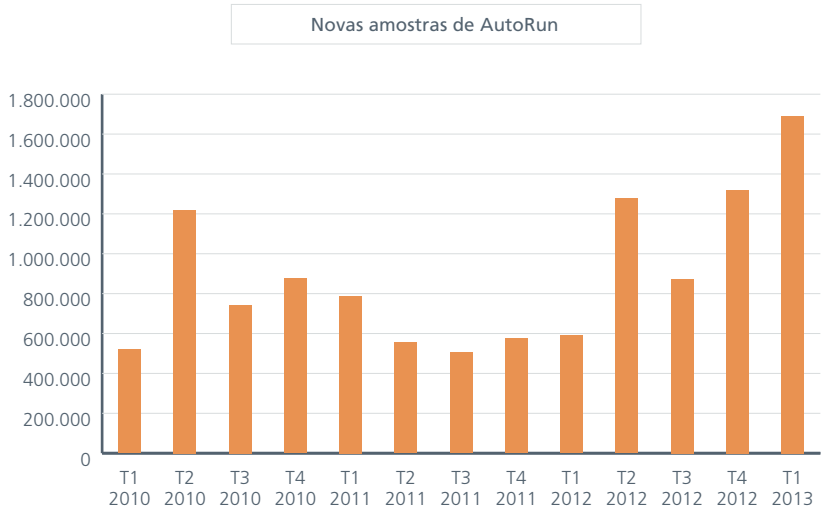
O McAfee Labs descobriu o primeiro aumento no volume global de spam em mais de três anos. E não foi um pequeno ressurgimento, pois o volume global de spam praticamente dobrou no primeiro trimestre de 2013. No entanto, o número global não é muito revelador, pois o McAfee Labs observou diferenças muito significativas no crescimento do spam em cada região. Novamente, os perpetradores parecem estar visando regiões específicas com fraudes específicas, na esperança de enganar novas vítimas. Fraudes populares no primeiro trimestre incluíram o retorno de esquemas de manipulação do mercado de ações e ofertas de drogas supostamente com hormônios de crescimento.



As descobertas de Koobface, um worm identificado pela primeira vez em 2008, que permaneceram relativamente estáveis no ano passado, *triplicaram* no primeiro trimestre de 2013, atingindo níveis nunca vistos. A comunidade cibercriminosa obviamente acredita que os usuários de mídias sociais constituem um ambiente repleto de vítimas em potencial.



A outra ameaça retrô que disparou no primeiro trimestre foram as novas amostras de malware AutoRun (de execução automática). Os worms AutoRun eram tradicionalmente distribuídos através de pen-drives USB ou CDs. Eles são particularmente úteis para os cibercriminosos porque podem ser utilizados para instalar backdoors ou ladrões de senhas nas máquinas infectadas. O pico em descobertas de AutoRun está, provavelmente, sendo impulsionado pela popularidade de serviços de compartilhamento de arquivos com base na nuvem.



Além desses ataques "De Volta para o Futuro", o McAfee Labs notou um crescimento significativo na técnica relativamente nova de ataques de "pilha de armazenamento". Mais conhecidos como ataques contra o registro mestre de inicialização (MBR), seu objetivo é infectar o sistema de armazenamento da máquina e, a partir daí, assumir o controle de todo o dispositivo. O surgimento de amostras de MBR aumentou mais de 30% no primeiro trimestre.

O que essas tendências significam para empresas que estão tentando otimizar sua postura de segurança? Para proteção de terminais, essa evolução do cenário de ameaças requer o uso de defesas em camadas que incluam não apenas um antivírus básico, mas também prevenção de intrusões e filtragem da Web. Devido ao aumento contínuo no uso de sites infectados para distribuição de malware, essas duas últimas funções nunca foram tão importantes. Em determinados ambientes, pode ser necessário adicionar também ferramentas de segurança para controle de aplicativos e dispositivos, para assegurar a proteção de informações de missão crítica residentes nos dispositivos dos usuários finais.

Além da proteção de terminais em camadas, é preciso equipar os administradores de segurança com ferramentas mais funcionais de geração de relatórios e resposta. Esse "cockpit de segurança" em evolução será cada vez mais importante para que os profissionais de segurança possam reagir rapidamente e efetivamente aos novos ataques direcionados emergentes.

A proteção de infraestruturas também exigirá uma abordagem em camadas que enfrente ameaças via Web, e-mail e rede. A melhor maneira de se proteger contra novas ameaças é interrompê-las antes que elas entrem na infraestrutura da empresa. No entanto, além dos esquemas padrão de proteção de perímetro, o uso crescente de serviços com base na nuvem requer que a postura de segurança da empresa seja estendida até a nuvem e implementada de maneira consistente, independente de onde os aplicativos e dados de missão crítica sejam distribuídos.

Uma cópia do relatório completo pode ser encontrada aqui:
http://www.mcafee.com/br/resources/reports/rp-quarterly-threat-q1-2013.pdf.

McAfee
An Intel Company

McAfee do Brasil Comércio de Software Ltda.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.mcafee.com/br