Sumário

1. O malware móvel será o impulsionador do crescimento, tanto na inovação técnica quanto no volume de ataques, do "mercado" total de malware em 2014.

Em 2013 a taxa de crescimento do surgimento de malware móvel novo, voltado quase exclusivamente para a plataforma Android, foi bem maior que a taxa de crescimento do malware novo voltado para PCs. Nos dois últimos trimestres pesquisados, o malware novo para PC manteve-se estável, enquanto o surgimento de novas amostras para Android cresceu em 33%.

Embora o McAfee Labs preveja que essa tendência continue em 2014, as novidades não se restringem à taxa de crescimento em novos ataques móveis. Também prevemos o aparecimento de ataques inteiramente novos contra Android. É altamente provável que testemunhemos os primeiros ataques autênticos de ransomware (vírus sequestrador) contra dispositivos móveis. O ransomware criptografa dados importantes no dispositivo e os retêm em troca de um resgate. As informações só serão liberadas se a vítima entregar uma quantia, seja em moeda convencional ou virtual (como Bitcoin) ao autor do ataque. Outras táticas novas que esperamos ver no âmbito da mobilidade incluem ataques contra vulnerabilidades em recursos de comunicação de curto alcance atualmente encontrados em muitos dispositivos, e ataques que corrompam aplicativos legítimos para fins de vazamento de dados sem detecção.

Os ataques contra dispositivos móveis também terão como alvo infraestruturas corporativas. Esses ataques serão viabilizados pelo fenômeno BYOD ("traga seu próprio dispositivo", do inglês "Bring Your Own Device"), atualmente comum, aliado à relativa imaturidade da tecnologia de segurança móvel. Os usuários que fizerem download de malware inadvertidamente introduzirão no perímetro corporativo malware desenvolvido para vazar dados confidenciais. O BYOD não é uma moda passageira, portanto, as corporações precisam implementar políticas e soluções abrangentes de gerenciamento de dispositivos para não se tornarem vítimas.

2. As moedas virtuais fomentarão ataques maliciosos de ransomware por todo o mundo.

Ataques do tipo ransomware, que criptografam dados nos dispositivos das vítimas, já não são novidade. Contudo, tais ataques têm sido sempre vulneráveis a investigações policiais realizadas contra as empresas utilizadas pelos atacantes para o processamento dos pagamentos.

Caixa de diálogo do CryptoLocker.

Embora o crescimento no uso de moedas virtuais beneficie e promova a atividade econômica, ele também proporciona aos cibercriminosos a perfeita infraestrutura de pagamentos anônima e desregulamentada de que eles precisam para coletar dinheiro de suas vítimas. Prevemos que ataques como o CryptoLocker proliferem enquanto tais ataques continuarem sendo (muito) lucrativos. Também esperamos ver novos ataques de ransomware voltados contra empresas que se propõem a criptografar dados corporativos essenciais.

A boa notícia, tanto para indivíduos quanto para empresas, é que embora a carga viral do ransomware seja específica, seus mecanismos de distribuição (spam, downloads de passagem e aplicativos infectados) não o são. Consumidores e empresas que mantiverem atualizados seus sistemas antimalware (tanto de terminais quanto de rede) estarão relativamente a salvo dessa ameaça. Um sistema de backup eficaz, distribuído individualmente ou em nível corporativo, também isolará as vítimas da maioria das consequências do ransomware.

3. Na corrida armamentista que caracteriza o mundo da guerra e do crime cibernéticos, quadrilhas criminosas e governos distribuirão novos ataques velados que serão cada vez mais difíceis de identificar e deter.

Conforme as soluções de segurança da informação tornam-se cada vez mais sofisticadas, aumenta também em sofisticação o empenho da comunidade cibercriminosa em contornar essas defesas. Os ataques que incluem técnicas avançadas de evasão representam a mais nova frente na guerra da segurança de dados corporativos. Uma técnica de evasão popular que será amplamente adotada pelos cibercriminosos em 2014 é a utilização de ataques com detecção de sandbox que não se distribuem completamente, a não ser que percebam que estão sendo executados em um dispositivo não protegido.

Outras tecnologias de ataque frequentemente utilizadas que serão ainda mais desenvolvidas e distribuídas em 2014 incluem ataques de programação orientada para retorno, que fazem com que aplicativos legítimos se comportem de maneiras maliciosas; malware que exclui a si próprio, cobrindo seus rastros após comprometer um alvo; e ataques avançados contra sistemas de controle industrial dedicados, que têm o potencial de danificar infraestruturas públicas e privadas.

Ataques com motivação política continuarão a aumentar, especialmente por ocasião das Olimpíadas de Inverno Sochi 2014 (em fevereiro) e a Copa Mundial da FIFA no Brasil (em junho e julho). Hacktivistas também aproveitarão esses eventos para promover suas ideias.

As organizações de TI corporativa precisarão reagir a esse novo conjunto de táticas para assegurar que suas defesas não dependam completamente de medidas de segurança que possam ser facilmente contornadas por quadrilhas cibercriminosos globais.

4. Os "ataques sociais" serão comuns até o final de 2014.

Ataques de plataforma social são aqueles que aproveitam as grandes bases de usuários do Facebook, Twitter, LinkedIn, Instagram, etc. Muitos desses ataques imitarão as táticas de malware tradicional, como o Koobface, e simplesmente utilizarão as plataformas sociais como mecanismo de entrega. Porém, também prevemos para 2014 ataques que empreguem características específicas das plataformas sociais para fornecer dados sobre atividades profissionais, localização ou contatos do usuário que possam ser utilizados para direcionar anúncios ou perpetrar crimes do mundo real ou virtual.

Um dos ataques de plataforma mais comuns simplesmente rouba credenciais de autenticação dos usuários e as utiliza para extrair dados pessoais de "amigos" e colegas incautos. A rede de bots Pony[1], que roubou mais de dois milhões de senhas de usuários do Facebook, Google, Yahoo e outros, é provavelmente apenas a ponta do iceberg. O próprio Facebook estima que 50 a 100 milhões de suas contas de usuário ativas por mês (MAU, do inglês "Monthly Active User") são duplicadas e que até 14 milhões de suas MAUs registradas são consideradas "indesejáveis". Segundo um recente estudo da Stratecast, 22% dos usuários de mídias sociais já passaram por algum incidente relacionado a segurança.[2]

Empresas, tanto públicas quanto privadas, também se valem de plataformas sociais para realizar "ataques de reconhecimento" contra seus concorrentes e rivais, seja diretamente ou através de terceiros. Líderes estabelecidos em ambos os setores público e privado foram alvo de tais ataques em 2013. Podemos esperar que a frequência e o alcance desses ataques sejam maiores em 2014.

A outra forma de ataque que prevemos em quantidade para 2014 são os ataques de "bandeira falsa" que induzem os usuários a revelar informações pessoais ou credenciais de autenticação. Um dos ataques mais populares apresentará uma solicitação "urgente" para que o usuário redefina sua senha. Em vez de fazer isso, ele roubará as credenciais de nome de usuário e senha e, então, utilizará a conta do usuário incauto para coletar informações pessoais sobre o usuário e seus contatos.

Evitar ambos os ataques de plataforma social e bandeira falsa exigirá mais vigilância por parte de indivíduos e políticas e soluções corporativas para assegurar que o uso das plataformas de mídia social não resulte em violações de dados concretas.

5. Novos ataques a computadores e servidores visarão vulnerabilidades acima e abaixo do sistema operacional.

Embora muitos grupos cibercriminosos se voltem para os dispositivos móveis, outros continuarão a visar as plataformas de computador e servidor. No entanto, os novos ataques que veremos em 2014 não vão apenas visar o sistema operacional, mas também explorar vulnerabilidades tanto acima quanto abaixo do SO.

Muitos dos novos ataques contra computadores em 2014 explorarão vulnerabilidades do HTML5, protocolo que viabiliza interação, personalização e recursos avançados para programadores. Porém, o HTML5 também expõe várias novas superfícies de ataque. Utilizando HTML5, pesquisadores já demonstraram como monitorar o histórico de navegação de um usuário para melhor contextualizar anúncios. Como muitos aplicativos baseados em HTML5 são desenvolvidos para dispositivos móveis, esperamos ver ataques que ultrapassem as fronteiras do navegador, dando aos atacantes acesso direto ao dispositivo e a seus serviços. Muitas empresas também criarão aplicativos corporativos baseados em HTML5. Para prevenir o vazamento dos dados utilizados por esses aplicativos, será necessário incorporar segurança nesses novos sistemas desde o início de sua utilização.

Os cibercriminosos estão cada vez mais visando vulnerabilidades abaixo do sistema operacional, na pilha de armazenamento e até mesmo no BIOS. No ambiente corporativo, debelar esses ataques de baixo nível exigirá a distribuição de medidas de segurança assistidas por hardware que também operem abaixo do nível do sistema operacional.

6. O cenário de ameaças em evolução determinará a adoção de análises de grandes volumes de dados de segurança para satisfazer os requisitos de detecção e desempenho.

Tradicionalmente, a maioria das soluções de segurança da informação depende de identificar cargas maliciosas (lista negra) ou rastrear aplicativos sabidamente válidos (lista branca). O atual desafio diante dos profissionais de segurança da informação envolve identificar e processar adequadamente as cargas que não se enquadram nesses extremos (cargas "cinza"). Isso requer a aplicação de múltiplas tecnologias de segurança em conjunto com serviços sólidos de reputação de ameaças.

Os serviços de reputação de ameaças já provaram seu valor na detecção de malware, sites maliciosos, spam e ataques de rede. Em 2014, os fornecedores de segurança acrescentarão novos serviços de reputação de ameaças e ferramentas de análise que permitirão a eles e a seus usuários identificar ameaças persistentes avançadas e ocultas mais rapidamente e com mais precisão do que se pode fazer hoje. Análises de grandes volumes de dados permitirão que os profissionais de segurança identifiquem ataques sofisticados que utilizem técnicas avançadas de evasão e ameaças persistentes que possam prejudicar processos de negócios de missão crítica.

7. A distribuição de aplicativos corporativos com base em nuvem criará novas superfícies de ataque que serão exploradas pelos cibercriminosos.

Willie Sutton, conhecido por ter roubado 100 bancos no início do século XX, teria afirmado que roubava bancos "porque é onde está o dinheiro".[3] As quadrilhas de cibercriminosos do século XXI terão como alvo aplicativos e repositórios de dados baseados em nuvem porque é onde os dados estão, ou onde em breve estarão. Isso pode ocorrer através de aplicativos de negócios que não tenham sido avaliados pela TI de acordo com políticas de segurança corporativa. Segundo um relatório recente, mais de 80% dos usuários de negócios utilizam aplicativos em nuvem sem o conhecimento ou o suporte da TI corporativa.[4]

Embora as vantagens funcionais e econômicas dos aplicativos baseados em nuvem sejam inegáveis, eles também expõem aos atacantes toda uma nova família de superfícies de ataque, como os hipervisores presentes em todos os data centers, a infraestrutura de comunicação múltipla implícita no serviços em nuvem e a infraestrutura de gerenciamento utilizada para prover e monitorar serviços de nuvem em larga escala. O problema para os profissionais de segurança corporativa é que quando um aplicativo corporativo migra para a nuvem, a organização perde visibilidade e controle sobre o perfil da segurança.

A perda de controle direto do perímetro de segurança corporativa constitui uma imensa pressão sobre administradores e líderes de segurança ao assegurar que os procedimentos operacionais e o contrato de usuário do provedor de nuvem garantam a implantação e a constante atualização das medidas de segurança necessárias para confrontar o cenário de ameaças em evolução. Grandes corporações podem ter condições de exigir que os provedores de nuvem implementem medidas de segurança consistentes com a postura de segurança corporativa. O mesmo não se aplica a consumidores menores de serviços baseados em nuvem, os quais precisarão examinar cuidadosamente o contrato de usuário frequentemente ambíguo no que se refere a segurança e propriedade dos dados. Novos serviços em nuvem também expõem novas superfícies de ataque até que os serviços atinjam um nível de maturidade que inclua a instrumentação e as contramedidas necessárias para garantir a segurança dos dados que eles devem proteger.

Sobre os autores

Este relatório foi preparado e redigido por Christoph Alme, Cedric Cochin, Geoffrey Cooper, Benjamin Cruz, Toralv Dirro, Paula Greve, Aditya Kapoor, Klaus Majewski, Doug McLean, Igor Muttik, Yukihiro Okutomi, François Paget, Craig Schmugar, Jimmy Shah, Ryan Sherstobitoff, Rick Simon, Dan Sommer, Bing Sun, Ramnath Venugopalan, Adam Wosotowsky e Chong Xu.

Sobre o McAfee Labs

O McAfee Labs é a maior fonte do mundo em pesquisa de ameaças, inteligência sobre ameaças e liderança em ideias sobre cibersegurança. A equipe de 500 pesquisadores do McAfee Labs coleta dados sobre ameaças de milhões de sensores nos principais vetores de ameaça — arquivos, Web, mensagens e redes. Em seguida, ela realiza análises de correlação de ameaças entre vetores e oferece inteligência sobre ameaças em tempo real para produtos de segurança de rede e terminais perfeitamente integrados através de seu serviço McAfee Global Threat Intelligence baseado em nuvem. O McAfee Labs também desenvolve tecnologias fundamentais para detecção de ameaças — como DeepSAFE, geração de perfis de aplicativos e gerenciamento de listas cinza —que são incorporadas no mais amplo portfólio de produtos de segurança do mercado.

Sobre a McAfee

A McAfee, uma subsidiária pertencente à Intel Corporation (NASDAQ: INTC), capacita as empresas, o setor público e os usuários domésticos a experimentar com segurança os benefícios da Internet. A empresa fornece soluções e serviços de segurança proativos e comprovados para sistemas, redes e dispositivos móveis em todo o mundo. Com sua visionária estratégia Security Connected, sua abordagem inovadora para a segurança aprimorada por hardware e a rede exclusiva do Global Threat Intelligence, a McAfee está sempre empenhada em manter seus clientes em segurança. www.mcafee.com.br

[1] http://blogs.mcafee.com/consumer/pony-botnet-steals-2-million-passwords

[2] Stratecast, "*The Hidden Truth Behind Shadow IT*" (A verdade oculta por trás da TI invisível), novembro de 2013. http://www.mcafee.com/br/resources/reports/rp-six-trends-security.pdf

[3] O próprio Sutton disse nunca ter dado a famosa declaração a ele creditada, e explicou que roubava bancos "porque gostava".

[4] Stratecast, "*The Hidden Truth Behind Shadow IT*" (A verdade oculta por trás da TI invisível), novembro de 2013. http://www.mcafee.com/br/resources/reports/rp-six-trends-security.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

60756rpt_threats-predictions_1213_fnl_ETMG