Relatório

Previsões sobre ameaças em 2012

Por McAfee® Labs™

Sumário

Quando uma organização de pesquisa de segurança faz previsões sobre ameaças futuras, essas previsões podem ou não se concretizar. É claro que achamos interessante colocar nossos chapéus de mágico para fazer previsões sobre o que pode acontecer nos próximos meses, mas será que as ameaças mudam tanto assim de um ano para o outro? Sob muitos aspectos, o ano que passou foi um ano de transformações. Mas essas transformações sinalizaram uma revolução ou uma evolução? Tivemos grandes mudanças nas áreas de ameaças móveis, hacktivismo, explorações do lado do cliente, explorações de mídias sociais e ataques direcionados. Muitas dessas mudanças e tendências vão continuar influenciando o cenário de ameaças por anos.

Quais mudanças o McAfee Labs espera encontrar nas ameaças do ano que vem? Nossa previsão é o surgimento de vários cenários novos, além de evoluções expressivas até nos vetores de ameaças mais estabelecidos:

- As ameaças industriais vão amadurecer e se segmentar.
- Os ataques a hardware incorporado vão se tornar mais amplos e profundos.
- O hacktivismo e o Anonymous vão se reinventar e evoluir.
- Os sistemas de moeda virtual sofrerão ataques mais abrangentes, e com mais frequência.
- Não teremos o ano da guerra cibernética, mas sim o ano *em prol* da guerra cibernética.
- O DNSSEC motivará o surgimento de novos vetores de ameaças às redes.
- O spam tradicional vai se "legalizar", e o spearphishing vai evoluir e se tornar o ataque de mensagens direcionadas.
- Os rootkits e as redes de bots móveis vão amadurecer e convergir.
- Autoridades de certificação falsas e certificados falsos vão corroer a confiança dos usuários.
- Avanços nos sistemas operacionais e na segurança vão motivar o surgimento da próxima geração de redes de bots e rootkits.

Agora que já preparamos o cenário, vamos conferir os detalhes!

Ameaças industriais

As ameaças às redes de infraestrutura industriais e nacionais atraíram muita atenção recentemente, e há uma ótima explicação para isso. Essa é uma das poucas áreas nas quais uma ameaça cibernética realmente põe em risco vidas e propriedades. Os sistemas industriais do tipo SCADA (supervisory control and data acquisition, ou sistemas de supervisão e aquisição de dados) são tão vulneráveis quanto qualquer outro sistema em rede. A grande diferença é que muitos desses sistemas não foram projetados para o ambiente em rede que o mundo continua adotando. O aumento da interconectividade de sistemas e dispositivos que não foram projetados para esse tipo de acesso é um desastre esperando para acontecer, visto que muitos sistemas SCADA são distribuídos em ambientes que não adotam práticas de segurança da informação. Ao que parece, conectar sistemas de infraestrutura crítica à Internet e gerenciá-los com software comum e amplamente disponível é uma prática comum. Todo software tem suas vulnerabilidades, mas os sistemas industriais de TI precisam de um planejamento mais sério em termos de arquitetura, projeto e implementação. Os invasores vão fazer uso dessa falta de preparação com frequência e êxito cada vez maiores em 2012, mesmo que com o único intuito de realizar chantagem ou extorsão. Se levarmos em conta os objetivos de muitos grupos hacktivistas, a possível união de objetivos políticos às vulnerabilidades dos sistemas de controle industrial (ICS, industrial controller systems) deve ser levada *muito* a sério.

O Stuxnet provou que código malicioso é capaz de gerar respostas físicas no mundo real.[1] Ataques recentes a empresas de fornecimento de água nos Estados Unidos provam que essa área interessa cada vez mais aos invasores. Quanto mais as atenções se voltam para os sistemas SCADA e de infraestrutura, mais a falta de segurança deles vem à tona. Acreditamos que essa falta de segurança levará a ameaças maiores, através de frameworks e kits de ferramentas de exploração, sem falar no aumento dos ataques a sistemas ICS de fornecimento de energia e outros serviços públicos. Sempre que um grupo visado exibe um ponto fraco, os invasores partem para cima dele.

Os invasores costumam atacar sistemas que possam ser comprometidos com sucesso, e como podemos ver, o ambiente de sistemas ICS está cheio de possíveis alvos. Os administradores desses sistemas devem ficar atentos aos eventos recentes. Chegou a hora de trabalhar extensivamente nos testes de penetração e no planejamento de respostas a emergências, que incluem componentes cibernéticos e diálogo com autoridades policiais em todos os níveis. Eles precisam perguntar a si mesmos: o que vai acontecer quando nós formos os alvos?

A ameaça interna: hardware incorporado

Os sistemas incorporados ganharam popularidade e importância nos últimos anos. De modo geral, eles são projetados para desempenhar uma função de controle específica dentro de um sistema maior, muitas vezes com requisitos de computação em tempo real. Eles costumam residir dentro de dispositivos completos, que incluem hardware e outras peças mecânicas. Historicamente, essa arquitetura era usada para atender às necessidades das indústrias de aviônica, transportes e energia, além das indústrias automotiva e de dispositivos médicos. Agora ela ganha cada vez mais espaço no mundo das empresas, das corporações e dos consumidores. GPS, roteadores, pontes de rede e muitos dispositivos eletrônicos recentes voltados para o consumidor têm funções e projetos incorporados.

Para explorar sistemas incorporados, o malware terá que atacar na camada de hardware. Esse tipo de especialização tem ramificações que vão além das plataformas incorporadas.

Cada vez mais, os criadores de malware desenvolvem malware que visa áreas mais baixas do sistema operacional. Muitas vezes os invasores tentam obter acesso de root em um sistema em seu nível mais baixo, que inclui o registro mestre de inicialização e até mesmo camadas do BIOS. Se os invasores conseguirem inserir código capaz de alterar a ordem de inicialização ou de carregamento do sistema operacional, eles terão maior controle e manterão acesso a longo prazo ao sistema e a seus dados. O controle do hardware é a terra prometida dos invasores sofisticados.

Como consequência dessa tendência, outros sistemas que usam hardware incorporado se tornarão suscetíveis a esses tipos de ataques. Já vimos código conceitual que visa o hardware incorporado de sistemas automotivos, médicos e de serviços públicos. Nossa expectativa é de que esses códigos de prova de conceito se tornem mais eficazes a partir de 2012.

Hacktivismo

O hacktivismo não é novidade, mas teve mais publicidade, aceitação e utilização do que nunca com o destaque dado à saga do WikiLeaks nos noticiários em 2010. De modo geral, 2011 foi um ano confuso para os ativistas on-line, com muitos conflitos internos e sem objetivos claramente definidos. Por muitas vezes foi difícil distinguir as campanhas com fins políticos das simples brincadeiras de jovens criadores de scripts em busca de diversão, mas uma coisa ficou clara: quando os hacktivistas escolhem um alvo, o alvo é comprometido por uma violação de dados ou negação de serviço. Não se deve subestimar a força dos hacktivistas. Mesmo que não concordemos com seus objetivos, o Anonymous e outros grupos hacktivistas provaram ser dedicados, cheios de recursos e até mesmo ágeis na escolha de alguns de seus alvos e operações.

O ano que vem será decisivo para o hacktivismo. E os casos envolvendo o Anonymous representam apenas um aspecto do problema.

- O "verdadeiro" Anonymous (ou seja, a ala histórica do grupo) vai reinventar o cenário do qual faz parte e a si mesmo, ou desaparecer. Se os círculos de influência do Anonymous não conseguirem se organizar, convocando seus integrantes a agir de maneira clara e assumindo a responsabilidade por essas ações, os hacktivistas que se dizem parte do Anonymous podem acabar sendo marginalizados. Seja como for, esse tipo de ataque vai crescer muito. O ataque de negação de serviço distribuído (DDoS, distributed denial of service) e a revelação de dados pessoais motivados por uma consciência política vão continuar crescendo.
- Aqueles que promovem a desordem digital vão se aproximar dos responsáveis por ataques que demonstram resultados físicos, no mundo real. Veremos mais casos de união entre o hacktivismo baseado em mídia social e o hacktivismo coordenado por mídia social. Nossa expectativa é de que as operações futuras incluam tanto componentes físicos quanto digitais. Ações conjuntas e coordenadas, no mundo real e on-line, serão planejadas simultaneamente. Não é difícil prever que o Occupy e outros grupos revoltosos vão evoluir e realizar ações digitais mais diretas. Como já comentamos em outras previsões, existe uma possibilidade muito concreta de que os objetivos dos hacktivistas se associem à disponibilidade dos sistemas SCADA e de controle industrial. Acreditamos que os hacktivistas linha-dura que apoiam os movimentos Occupy ao redor do mundo abandonarão o Anonymous, passando a operar como "Cyberoccupiers" (ocupantes cibernéticos).
- Em nome de objetivos políticos e ideológicos, a vida pessoal de figuras públicas, como políticos, líderes da indústria, juízes e agentes da lei e da segurança, será revelada com mais frequência do que em anos anteriores. Os manifestantes não vão poupar esforços para obter de redes sociais e servidores da Web dados que contribuam com suas operações.

- Alguns hacktivistas vão operar de forma semelhante aos diversos "exércitos cibernéticos" que se desenvolvem principalmente em estados não democráticos ou não seculares (como o Exército Cibernético do Irã, o Exército Cibernético do Paquistão, o grupo ChinaHonker etc). Esses exércitos, que nos últimos dois anos vinham se concentrando principalmente em ações de adulteração, passarão a realizar ações mais problemáticas no ano que vem. Alguns desses grupos vão entrar em conflito, o que pode acabar gerando danos colaterais imprevisíveis (palestinos contra israelenses, indianos contra paquistaneses, norte-coreanos contra sul-coreanos etc). Em 2011, rumores diziam que os exércitos cibernéticos eram manipulados ou apoiados por seus respectivos governos. Estados totalitários irão ainda mais longe no ano que vem, chegando ao ponto de reconhecer as ações de exércitos cibernéticos locais.

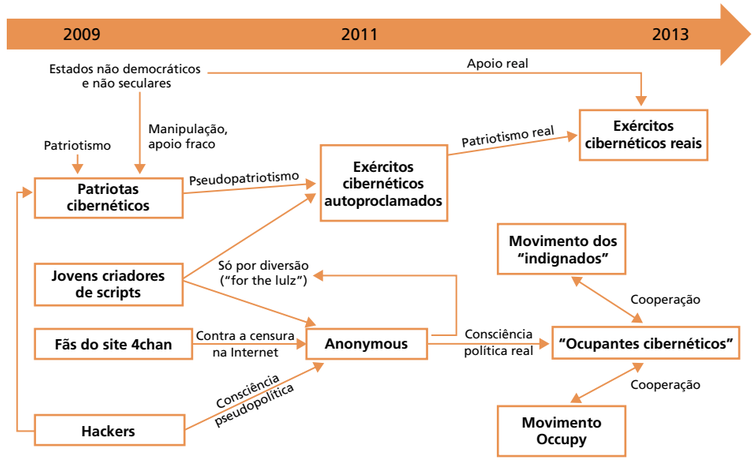

Figura 1. As muitas conexões e motivações do hacktivismo.

Moeda virtual

A moeda virtual, ou moeda cibernética, tornou-se uma forma popular de envio e recebimento de dinheiro on-line. Mesmo não se apoiando necessariamente em ativos ou mercadorias tangíveis, serviços como o Bitcoin permitem que os usuários façam transações por meio de uma rede ponto a ponto (peer-to-peer) descentralizada. Basicamente, trata-se de dinheiro eletrônico para pagamentos diretos e on-line. O usuário só precisa do software cliente e de um serviço de carteira on-line para receber "moedas", que são armazenadas na carteira e podem ser transferidas para outras pessoas como pagamento por bens ou serviços. Para enviar ou receber essas moedas, o usuário só precisa de um endereço de carteira. Percebeu o problema e a oportunidade?

O malware do tipo cavalo de Troia se encaixa facilmente nessa arquitetura. As carteiras não são criptografadas, e as transações são públicas. Para os criminosos cibernéticos, esse é um alvo atraente. Vários eventos de destaque relacionados às moedas virtuais ocorreram em 2011:

- O banco de dados do Mt. Gox Bitcoin Exchange (casa de câmbio de Bitcoins) foi alvo de invasores, que roubaram milhares de Bitcoins.
- Houve distribuição de spam promovendo ferramentas falsas de garimpagem de Bitcoins. Na verdade, essas ferramentas continham malware que enviava os arquivos da carteira da vítima para um local remoto. Elas também permitiam que outros garimpeiros usassem o computador infectado para continuar garimpando Bitcoins.
- Redes de bots de garimpeiros de Bitcoins foram encontradas em operação. Usando uma grande quantidade de máquinas infectadas, essas redes de bots eram capazes de acelerar a garimpagem e o processamento de Bitcoins, além de lançar ataques de DDoS.

A natureza de moedas e tecnologias virtuais como o Bitcoin torna esses alvos irresistíveis para os criminosos cibernéticos. Vimos um crescimento expressivo de malware direcionado a essas tecnologias em 2011. Vejamos, por exemplo, o malware voltado especificamente para o Bitcoin:

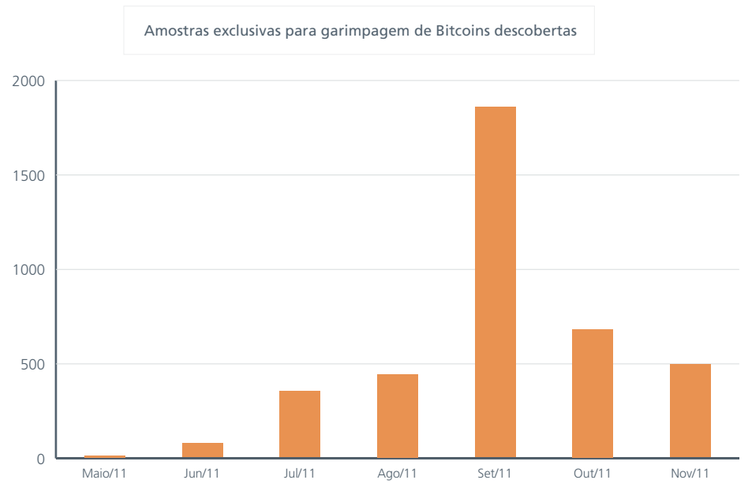

Figura 2. O roubo (também chamado de garimpagem) da moeda virtual Bitcoin atingiu seu ápice em setembro. A previsão é de que essa atividade aumente em 2012.

Nossa expectativa é de que essa ameaça evolua e se transforme em uma pequena indústria de crime cibernético no ano que vem, com spam, roubo de dados, ferramentas, redes de suporte e outros serviços associados, dedicando-se exclusivamente à exploração de moedas virtuais. Está claro que os criminosos cibernéticos encontraram um sistema de pagamentos adequado às suas necessidades.

Guerra cibernética

Será que 2012 vai ser o ano da guerra cibernética ou apenas uma vitrine para a exibição das armas de ataque cibernético e seu potencial? É óbvio que torcemos pela segunda opção, mas o crescimento dessa situação nos últimos anos faz com que uma eventual guerra cibernética seja quase inevitável. Temos visto técnicas "cibernéticas" sendo usadas com frequência para complementar métodos tradicionais de operações de inteligência (ou espionagem), com acusações trocadas entre parceiros e rivais. Essa é uma forma muito barata de espionagem, que sempre abre espaço para negações plausíveis, não põe vidas humanas em risco, e o que é mais importante, parece muito eficiente. O que não temos visto muito é o uso dessas técnicas como parte do arsenal de um conflito armado. Até o momento, só vimos isso acontecer em escala bem pequena, com ataques de sofisticação muito limitada, como por exemplo, no conflito na Geórgia.

Mas agora a situação mudou. Muitos países já perceberam o potencial incapacitante dos ataques cibernéticos a infraestruturas críticas, e como é difícil se defender deles. Esse potencial cria oportunidades para que pequenos países e organizações realizem ataques, especialmente quando esses países e organizações não possuem muitos alvos que possam ser contra-atacados. O ataque do Stuxnet foi um evento que mudou a situação em muitos aspectos. Ele deixou absolutamente claro para todos que a ameaça é real, e o impacto que esses ataques podem ter.

Os Estados Unidos sabem que provavelmente são o país mais vulnerável de todos, devido à sua grande dependência de sistemas de computadores e a uma defesa cibernética que praticamente só defende as redes do governo e dos militares. Imagine um exército que só protege as bases militares, e não o resto do país. Depois de ser muito criticado por não apresentar uma doutrina formal, o país finalmente reagiu.

Em julho, o relatório "Department of Defense Strategy for Operating in Cyberspace" (Estratégia do Departamento de Defesa para operações no ciberespaço) foi publicado.[2] Eis um trecho desse relatório (tradução livre): "Iniciativa estratégica 1: o DoD (Departamento de Defesa) tratará o ciberespaço como um domínio operacional para organizar, treinar e equipar de modo que o DoD possa tirar proveito máximo do potencial do ciberespaço." Mas o documento não trata de um assunto sobre o qual já discutimos: que os ataques cibernéticos podem motivar contra-ataques se tiverem impacto suficiente. Em vez disso, o DoD está preparando uma nova doutrina para complementar a estratégia cibernética, oferecendo orientações concretas à equipe de guerra cibernética do DoD. Mesmo que essa doutrina descreva em quais circunstâncias uma retaliação cibernética pode ser considerada, seu impacto nem de longe será tão profundo quanto o da doutrina da "ameaça de aniquilação total" que ajudou o mundo a sobreviver à guerra fria.

Ela não vai impedir ninguém de atacar se a possível resposta for confidencial e, portanto, desconhecida.

Relatos indicam que o uso de armas cibernéticas na revolução da Líbia foi considerado, mas não aconteceu porque ninguém queria ser o primeiro a abrir essa caixa de Pandora. Ou talvez não existissem muitos alvos no local. Por enquanto, porém, não tivemos demonstrações públicas da capacidade que a guerra cibernética ofensiva tenha de deter alguém. A pressão para que essas informações sejam trazidas a público está aumentando, e a expectativa é de que haja algum tipo de demonstração que vá além de vídeos assustadores que mostrem a diplomatas estrangeiros máquinas parando de funcionar. Uma demonstração eficaz tem potencial para gerar uma reação em cadeia, com outros estados mostrando que também podem usar os mesmos recursos.

Esperamos que o ano que vem só traga demonstrações, e não os efeitos de uma guerra cibernética real!

DNSSEC

O DNSSEC (Domain Name System Security Extensions, extensões de segurança do sistema de nomes de domínio) é uma tecnologia voltada para a proteção dos serviços de resolução de nomes contra falsificação e envenenamento de cache. Para isso, é utilizada uma "rede de confiança" com base em criptografia de chave pública. A intenção é proteger um computador cliente de comunicações não intencionais com um host, resultantes de um ataque de interceptação que redirecione o tráfego do servidor desejado (uma página da Web, e-mail etc) para outro servidor. Para proteger os usuários on-line e dificultar as coisas para os hackers, essa é uma etapa extremamente importante na evolução da Internet.

Infelizmente, o DNSSEC também impede que as autoridades usem falsificação e redirecionamento para reencaminhar tráfego da Internet destinado a sites que trafiquem imagens ou software ilegais. Para que o governo possa redirecionar o tráfego, ele teria que ser considerado uma autoridade nos domínios de nível raiz. Outros órgãos governamentais hesitariam em oferecer esse nível de confiança aos governos se soubessem que o resultado poderia ser a exclusão de conteúdo da Internet com base nas opiniões de governos estrangeiros.

As tentativas recentes de aprovar uma legislação que impeça o custeio de propriedade intelectual se baseiam em um entendimento do estado atual de funcionamento do DNS, e não do funcionamento futuro do DNSSEC. Essa lacuna pode criar mais requisitos legais para o gerenciamento da infraestrutura atual de DNS, e eles podem não ser compatíveis com a infraestrutura de DNSSEC. Se esses requisitos forem implementados, o processo de atualização de segurança de nossa infraestrutura de DNS pode ficar estacionado enquanto os comitês buscam um meio termo entre a lei e o DNSSEC.

Com órgãos governamentais de todo o mundo se mostrando mais interessados em estabelecer um "código de conduta" para o tráfego da Internet, nossa expectativa é de que cada vez mais as soluções do futuro sejam prejudicadas por disputas legislativas relacionadas a problemas do passado. Como resultado, a Internet do futuro provavelmente vai ser parecida com a Internet do passado por mais tempo do que nós, que trabalhamos com segurança, gostaríamos.

O spam vai se legalizar

Nos últimos quatro anos, houve um aumento na compreensão e na cooperação internacional para o combate ao spam ligado a redes de bots. Essa cooperação resultou na desativação de várias infraestruturas de grande destaque, essenciais para o controle de redes de bots (como o provedor de serviços de Internet McColo), a hospedagem de domínios de spam na Web (Glavmed) e o processamento de cartões de crédito vinculado a medicamentos falsificados. Além disso, processos foram abertos contra grandes corporações da Internet que ofereciam meios publicitários para atividades ilegais. Essas ações levaram a uma enorme queda nos volumes de spam global desde seu auge no meio de 2009, e elevaram consideravelmente os custos do mercado negro para o envio de spam através de redes de bots.

Essas ações não representam de forma alguma o fim de todo o spam, como alguns profetas da tecnologia andaram prevendo, mas mudam o cenário. Quando olhamos a situação atual, vemos cada vez mais spam não solicitado sendo enviado não por hosts infectados por redes de bots, mas por agências de propaganda "legítimas", que usam técnicas altamente criticadas pela comunidade antispam. As ações dessas agências fazem com que os endereços de e-mail dos usuários entrem em listas de anunciantes sem o conhecimento e o consentimento desses usuários. As técnicas para esse fim incluem a compra vergonhosa de listas de endereços de e-mail que afirmam incluir usuários que já consentiram em receber todo tipo de propaganda (e é preciso algum esforço mental para acreditar nisso). Também há o processo de "e-pending", que coleta endereços de e-mail através de algoritmos que determinam que esses usuários aceitariam receber propagandas se lhes fosse pedida permissão, e que portanto pula a parte de pedir permissão, incluindo-os diretamente, sem pedir nada. Há ainda a compra de bancos de dados de clientes de empresas que encerram atividades e ignoram a política de privacidade vigente quando a empresa atuava, e as "parcerias" com outras entidades publicitárias ou provedores de listas de discussão para entupir suas listas de e-mail com propaganda.

As empresas de publicidade que fazem isso sabem que estão enviando spam, e empregam as mesmas técnicas que operadores de redes de bots usam para fugir à detecção. Todo dia, milhares de novos domínios de e-mail são registrados usando a privacidade do whois para evitar a identificação de seu proprietário. Milhares de novos endereços IP são ativados nas sub-redes de provedores de hospedagem para que o canhão do spam abra fogo por algumas horas contra as caixas de entrada, usando e-mails mal formatados, cheios de erros de ortografia e gramática desastrosa. A maioria desses e-mails contém um link para remover o endereço da lista, mas o link só serve para que o spammer saiba que seu endereço está ativo e que você leu o e-mail dele. E às vezes há endereços físicos para os quais você pode mandar uma carta pedindo para ser removido da lista, mas uma pesquisa on-line revela que esses endereços vão de cabanas nas regiões inóspitas do Canadá a regiões áridas no deserto do Arizona. Em alguns casos, endereços de e-mail individuais recebem mais de 9.000 mensagens de spam praticamente idênticas no mesmo dia, anunciando os benefícios à saúde oferecidos por um popular bracelete magnético.

Essas práticas corruptas de publicidade têm o apoio da lei. A lei CAN-SPAM, dos Estados Unidos, foi tão amenizada que quem faz propaganda não precisa de permissão para enviar publicidade. Como a propaganda é um negócio muito lucrativo e altamente influenciado por lobbies, é extremamente improvável que vá ocorrer qualquer mudança significativa nas práticas de gerenciamento de listas de e-mails, ou que alguma penalidade expressiva vá ser aplicada.

Nesse ambiente, a expectativa é de que o spam legalizado continue crescendo em ritmo alarmante. É mais barato e menos arriscado enviar spam por meio de empresas de publicidade do que usando hosts infetados por redes de bots. Essa prática, conhecida como "snowshoe spamming", cresceu tanto que até o momento os dez assuntos mais comuns em e-mails incluem uma notificação de status de entrega, um spam de uma rede de bots sobre relógios Rolex falsificados, uma fraude de confiança e sete assuntos associados a spam do tipo snowshoe. Esse tipo de tráfego vai continuar crescendo em ritmo mais acelerado que o phishing e as fraudes de confiança. Enquanto isso, o spam vindo de redes de bots vai continuar caindo conforme os donos desses bots forem encontrando maneiras mais seguras de obter dinheiro de seus exércitos de computadores infectados. É questão de tempo até que a maior parte do volume de spam global venha de entidades de péssima postura, porém legalizadas.

Ameaças móveis

Nos últimos dois anos, os ataques a smartphones e dispositivos móveis aumentaram. Lidamos com rootkits, redes de bots e outros tipos de malware. Os invasores abandonaram o malware simples e destrutivo em prol de spyware e malware que rendem dinheiro. Eles exploraram vulnerabilidades para burlar as proteções dos sistemas e obter maior controle sobre os dispositivos móveis. Em 2012, acreditamos que os invasores vão continuar fazendo a mesma coisa, só que aprimorando seus ataques. Também prevemos que o foco dos ataques vá mudar para operações bancárias em dispositivos móveis.

Redes de bots + rootkits = problemas de baixo nível

Nos PCs, os rootkits e as redes de bots distribuem propagandas que geram dinheiro às custas das vítimas. Nos dispositivos móveis, notamos um uso semelhante desses tipos de malware. Os rootkits permitem a instalação de mais software ou spyware, e as redes de bots podem gerar cliques em anúncios ou enviar mensagens de texto com tarifas especiais.

Encontramos variantes móveis de famílias de malware que incluem Android/DrdDream, Android/DrdDreamLite e Android/Geinimi, além de Android/Toplank e Android/DroidKungFu. Alguns desses tipos de malware usam explorações de "root" (desenvolvidas originalmente para que os clientes desbloqueiem seus próprios telefones) para obter acesso e assumir o controle dos telefones das vítimas. No ano que vem, conforme os desenvolvedores e pesquisadores desenvolverem novos métodos de rooting para telefones, veremos os criadores de malware adaptarem as lições aprendidas com o desenvolvimento de malware para PCs. A intenção deles será a de realizar ataques que tirem maior proveito da camada de hardware dos dispositivos móveis. O malware baseado em PCs está "descendo" cada vez mais no sistema operacional para tirar mais proveito do hardware. Nossa expectativa é de que o malware para dispositivos móveis trilhe o mesmo caminho.

Os bootkits, um tipo de malware que substitui ou ignora a inicialização do sistema, também ameaça os dispositivos móveis. O rooting de um telefone ou leitor de e-books permite a adição de novos recursos ou a substituição do sistema operacional do dispositivo. Por outro lado, ele também pode permitir que invasores carreguem seus próprios sistemas operacionais modificados. Um rootkit para dispositivos móveis apenas modifica o sistema operacional existente para evitar a detecção, mas um bootkit pode dar ao invasor muito mais controle sobre o dispositivo.

Por exemplo, o kit de ferramentas "Weapon of Mass Destruction", usado em testes de penetração de dispositivos móveis, opera em telefones antigos com o Windows Mobile. O WMD se instala usando ferramentas desenvolvidas para carregar o Linux em telefones com o Windows Mobile, e permite ao usuário reinicializar o sistema operacional original. Os invasores já usam explorações de root antigas para se ocultar; com o desenvolvimento de novas explorações, mais cedo ou mais tarde eles instalarão seu próprio firmware personalizado.

Ataques a operações bancárias móveis

Os usuários de PCs já conhecem os ataques de criminosos que usam kits de crimeware como o Zeus e o SpyEye para roubar dinheiro de contas bancárias on-line. Tanto o Zeus quanto o SpyEye começaram a usar aplicativos móveis como auxiliares para burlar a autenticação de dois fatores e obter acesso ao dinheiro da vítima.

O Zitmo (Zeus-in-the-mobile) e o Spitmo (SpyEye-in-the-mobile) são duas famílias de spyware móvel que encaminham mensagens SMS para os invasores. Para usar esse spyware, os invasores precisavam fazer login manualmente para roubar o dinheiro dos usuários.

Em julho, o pesquisador de segurança Ryan Sherstobitoff explicou como as transações realizadas por criminosos usando o Zeus e o SpyEye poderiam ser rastreadas, visto que eram totalmente diferentes das transações feitas por usuários legítimos. No mês passado, ele mostrou como os criminosos se adaptaram. Agora, eles são capazes de roubar dados das vítimas de forma programática, enquanto elas ainda estão conectadas. Isso contribui para que as transações dos criminosos pareçam vir de usuários legítimos. A adição de um atraso na transação faz com que ela pareça estar sendo realizada por um humano. Os invasores se adaptam rapidamente a todas as mudanças realizadas para a proteção das operações bancárias nos PCs. E quanto mais usarmos nossos dispositivos móveis para realizar operações bancárias, mais os invasores vão deixar os PCs de lado para investir diretamente em aplicativos voltados para esse tipo de operação. Acreditamos que os ataques que tiram proveito desse tipo de técnica programática vão se tornar mais frequentes conforme o número de usuários que cuidam de suas finanças em dispositivos móveis aumentar.

Certificados falsificados

Nós geralmente acreditamos em arquivos e documentos assinados digitalmente, porque confiamos nas assinaturas digitais e nas autoridades de certificação que as emitem. Muitos sistemas de controle de aplicativos e criação de listas brancas dependem de assinaturas digitais válidas. Essas soluções nos permitem criar políticas e controles para lidar com serviços, aplicativos e até arquivos que contenham uma assinatura digital válida. A navegação e as transações comerciais seguras pela Web também dependem de assinaturas digitais confiáveis. Essas autoridades de certificação e seus certificados basicamente dizem ao sistema operacional, "pode confiar em mim, minha validade foi comprovada".

Mas com tanta confiança, o que acontece se nos depararmos com certificados digitais falsos? Ou indo além, quais são as implicações do comprometimento de uma autoridade de certificação? Os certificados digitais nos oferecem um certo grau de confiança em um arquivo, processo ou transação. Produzindo e distribuindo certificados falsos, os invasores podem realizar ataques quase indetectáveis. No navegador, isso permite que o invasor realize ataques de interceptação: o tráfego que deveria estar criptografado e ser invisível ao invasor agora pode ser visto como texto puro, porque ele tem a "chave". No host, o software de segurança ignora arquivos assinados com uma chave válida, já que agora eles aparentemente estão na lista branca: eles têm acesso autorizado, graças ao certificado que apresentam.

Ameaças recentes, como o Stuxnet e o Duqu, usaram certificados falsos para evitar a detecção, obtendo ótimos resultados. Não foi a primeira vez que vimos esse tipo de comportamento (usado anteriormente por antivírus falso, por variantes do Zeus, pelo Conficker e até por alguns tipos antigos de malware para o Symbian), mas nossa expectativa é de que essa tendência aumente a partir de 2012.

A maior ameaça, que seria o ataque a autoridades de certificação para a produção de certificados falsos, também é algo preocupante para o futuro. Esse tipo de comprometimento permitiria a um invasor criar várias chaves, que poderiam ser usadas em diversos cenários com base na Web e com base em hosts, acabando com boa parte da confiança integrada a um sistema operacional. Nós estamos muito preocupados com as implicações do uso em larga escala de certificados falsos nas tecnologias de controle de aplicativos e criação de listas brancas que usam esses certificados. A DigiNotar, uma autoridade holandesa de certificação que já passava por problemas, declarou falência recentemente após uma violação de segurança que resultou na emissão de certificados fraudulentos. Será que esse ataque foi o último prego no caixão da DigiNotar? As investigações mostram que até 531 certificados fraudulentos foram emitidos pela DigiNotar. A ruína da empresa provavelmente é só a primeira de várias histórias que ainda vamos ouvir sobre violações nesse setor. Agora, temos que determinar a extensão dos danos e do comprometimento da confiança.

O ataque em larga escala a autoridades de certificação e o uso mais abrangente de certificados digitais fraudulentos, porém válidos, têm ramificações que afetam a infraestrutura de chaves públicas, a navegação segura e as transações, além de tecnologias com base em hosts, como o controle de aplicativos e a criação de listas brancas. Tirar proveito de nossa confiança nesse sistema dá uma grande vantagem aos invasores, portanto acreditamos que eles vão se concentrar nessa área.

Avanços nos sistemas operacionais

A segurança da informação é um eterno dar e receber, com medidas e contramedidas sendo aplicadas em doses iguais. Os invasores criam código malicioso, e nós contra-atacamos. Os fornecedores de sistemas operacionais incluem segurança no núcleo do sistema operacional, e os invasores acham um jeito de subvertê-la. Isso é algo natural no cenário dinâmico de ameaças, e nunca vai mudar. Mas será que os avanços trazidos pelo setor de segurança da informação e pelos fornecedores de sistemas operacionais farão com que os criadores de malware esqueçam o sistema operacional e ataquem o hardware diretamente?

Versões recentes do Windows incluem proteção contra execução de dados e aleatorização do espaço de endereços. Esses métodos de segurança dificultam o comprometimento da máquina da vítima pelos invasores. Nos últimos anos, as tecnologias de criptografia também aumentaram a proteção do sistema operacional. Assim como acontece com a maioria das medidas internas de segurança do sistema operacional, os invasores não demoraram para descobrir maneiras de burlar essas tecnologias. Com o futuro Windows 8, a Microsoft incluirá muitos recursos novos de segurança: armazenamento seguro de senhas, funções de inicialização segura, defesas antimalware e até recursos aprimorados de reputação. Para onde essa nova arquitetura de segurança vai levar os invasores?

A resposta é: para dentro do hardware, e para fora do sistema operacional.

Nos últimos anos, o McAfee Labs presenciou grandes avanços nos rootkits e bootkits dos invasores e criadores de malware. Os rootkits são usados para subverter o sistema operacional e o software de segurança. Já os bootkits atacam a criptografia, e podem substituir carregadores de inicialização legítimos. Essas são técnicas avançadas para interceptar chaves de criptografia e senhas, e até mesmo para subverter as defesas de assinaturas de drivers de alguns sistemas operacionais.

Não é fácil atacar o hardware e o firmware, mas quando dá certo os invasores podem criar "imagens" de malware persistentes em placas de rede, discos rígidos e até no BIOS do sistema. Ao longo de 2012 e além dele, acreditamos que o trabalho em explorações de hardware e firmware, e em seus ataques relacionados no mundo real, vá se intensificar.

O Windows 8 nem foi lançado ainda, e pesquisadores já demonstraram como usar BIOS legado para subverter os avanços do recurso de segurança do carregador de inicialização. Com o maior desenvolvimento das especificações da interface de firmware extensível e unificada da Intel, projetada para ser uma interface de software entre o sistema operacional e o firmware da plataforma para garantir uma inicialização segura e substituir o BIOS legado, a expectativa é de que mais invasores se dediquem a pesquisar técnicas de evasão nos próximos anos.

Vamos observar atentamente como os invasores farão uso dessas funções de baixo nível para o controle de redes de bots, talvez migrando suas funções de controle para funções do processador gráfico, o BIOS ou o registro mestre de inicialização. Também acreditamos que os invasores aproveitarão protocolos "novos" como o IPv6 conforme as implementações de rede avançarem nos moldes dos sistemas operacionais.

Apesar de nossos esforços em frustrar suas ambições, os invasores entendem claramente o valor e o poder de atacar o hardware e abandonar os ataques tradicionais ao sistema operacional.

Sobre os autores

Este relatório foi preparado e escrito por Zheng Bu, Toralv Dirro, Paula Greve, David Marcus, François Paget, Ryan Permeh, Craig Schmugar, Jimmy Shah, Peter Szor, Guilherme Venere e Adam Wosotowsky do McAfee Labs.

Sobre o McAfee Labs

McAfee Labs é o grupo de pesquisa global da McAfee. Com a única organização de pesquisa dedicada a todos os vetores de ataque — malware, Web, e-mail, redes e vulnerabilidades — o McAfee Labs reúne informações de seus milhões de sensores e de seu serviço com base na nuvem, o McAfee Global Threat Intelligence™. Os 350 pesquisadores multidisciplinares do McAfee Labs em 30 países acompanham toda a gama de ameaças em tempo real, identificando vulnerabilidades em aplicativos, analisando e correlacionando riscos e permitindo correções instantâneas para proteger as empresas e o público.

Sobre a McAfee

A McAfee, uma subsidiária pertencente à Intel Corporation (NASDAQ:INTC), é a maior empresa do mundo dedicada à tecnologia de segurança. A McAfee provê soluções proativas e com qualidade comprovada, além de serviços que ajudam a manter sistemas, redes e dispositivos móveis protegidos mundialmente, permitindo aos usuários conectarem-se à Internet, navegarem e realizarem compras pela Web com segurança. Apoiada pelo incomparável centro Global Threat Intelligence, 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, prevenir interrupções, identificar vulnerabilidades e monitorar continuamente dados, além de incrementar a segurança em TI. A McAfee protege o seu mundo digital. O compromisso maior da McAfee é encontrar constantemente novas maneiras de manter nossos clientes seguros. http://www.mcafee.com/br

[1] https://blogs.mcafee.com/mcafee-labs/stuxnet-update
[2] A versão pública pode ser lida em http://www.defense.gov/news/d20110714cyber.pdf

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

40302rpt_threat-predictions_1211_fnl_ETMG