White paper

Como lidar com a sequência de ataque completa: antes, durante e depois de um ataque

É hora de ter um novo modelo de segurança

O panorama de ameaças de hoje é muito diferente daquele de apenas 10 anos atrás. Ataques simples que causavam danos que podiam ser contidos deram espaço a operações modernas de crime cibernético que são sofisticadas, bem financiadas e capazes de causar grandes problemas a empresas e à infraestrutura nacional. Além de esses ataques avançados serem difíceis de detectar, eles também permanecem nas redes por longos períodos e acumulam os recursos de rede para fazer ataques em outro lugar.

As defesas tradicionais que dependem exclusivamente de detecção e bloqueio para proteção não são mais adequadas. É hora de termos um novo modelo de segurança que lide com a sequência de ataque completa: antes, durante e depois de um ataque.

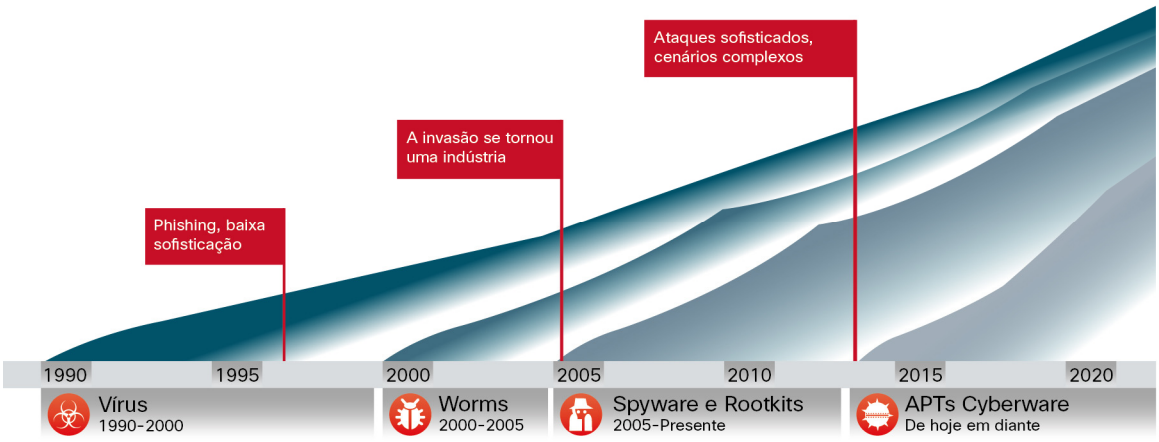
A industrialização da invasão

Os primeiros vírus de PC surgiram há mais de 25 anos. Nós nem imaginávamos que eles eram apenas o início do que se tornaria a industrialização da invasão.

Por quase 10 anos, os vírus resistiram como o método principal de ataque, e com o tempo foram vencidos especialmente pela capacidade de bloqueio e proteção dos defensores. Movidos pela fama e conhecimento obtidos através da detecção e divulgação das novas vulnerabilidades, os invasores continuaram a inovar. O que se seguiu foram ciclos de ameaça distintos, uma “corrida armamentista”, por assim dizer. Aproximadamente a cada cinco anos, os invasores lançariam novos tipos de ameaças, de vírus de macro a worms, spywares e rootkits, e os defensores inovariam rapidamente para proteger as redes contra eles.

Não é de admirar que possamos mapear esses ciclos nas grandes mudanças na tecnologia que apresentaram novos vetores de ataque (consulte a Figura 1). Os primeiros vírus tinham o sistema operacional como principal alvo e eram propagados pela rede-peão (“sneaker net”). Os vírus de macro aproveitavam o compartilhamento de arquivos pelos usuários. As ameaças de worms que passavam de uma máquina para outra utilizavam as redes empresariais e o uso cada vez maior da Internet. Os spywares e os rootkits vieram com o surgimento de novos aplicativos, dispositivos e comunidades online. Hoje, nos deparamos com malwares avançados, ataques direcionados e ameaças persistentes avançadas (APTs, advanced persistent threats). O que diferencia a era atual da anterior são as motivações e as ferramentas envolvidas nos ataques, que os tornam especialmente difíceis de serem detectados, compreendidos e interrompidos.

Figura 1. A industrialização da invasão



A industrialização da invasão está criando uma geração de lucros da economia criminosa mais rápida, eficaz e eficiente a partir dos ataques a nossa infraestrutura de TI. A troca organizada de explorações é próspera e lucrativa, e o mercado aberto ajuda a impulsionar a mudança da exploração para roubo, transtorno e destruição. E, como os criminosos cibernéticos descobriram que há muito dinheiro em jogo, o trabalho deles ficou mais padronizado, mecanizado e orientado por processo. Como os invasores conhecem a natureza estática das tecnologias clássicas de segurança e suas diferentes implantações, eles conseguem explorar as lacunas existentes entre elas e suas vulnerabilidades. É até muito comum que grupos de hackers acompanhem os processos de desenvolvimento de software, como a realização de testes de garantia de qualidade e testes de bancada nos produtos em relação às tecnologias de segurança antes da sua liberação, para ajudar a garantir que eles continuarão evitando proteções comuns.

Agora, há incentivos financeiros significativos para a manutenção do sigilo, e muitos grupos de “hackers ativistas” estão entusiasmados para lançar ataques que resultem em ganho político ou econômico com pouca probabilidade de represálias ou processos judiciais. Novos métodos, como salto de porta e protocolo, tunelamento criptografado, droppers, bem como ameaças combinadas e técnicas que usam engenharia social e ataques de dia zero deixaram a entrada dos hackers mais fácil, rápida e econômica e dificultam cada vez mais o trabalho dos defensores de identificá-los e afastá-los. Para piorar essa indefinição, os próprios ataques podem mudar rapidamente à medida que avançam na empresa em busca de uma posição de destaque e extraindo dados importantes.

O desafio Any-to-Any

Redes modernas ampliadas e seus componentes desenvolvem-se constantemente e geram novos vetores de ataque. Esses incluem dispositivos remotos, aplicativos remotos e habilitados pela Web, hipervisores, mídia social, navegadores da Web e computadores incorporados, bem como uma proliferação de dispositivos e serviços que ainda nem conhecemos, trazidos pela Internet de Todas as Coisas. As pessoas estão dentro e fora da rede, em qualquer dispositivo, acessando qualquer aplicativo e em muitas nuvens diferentes. Essa onipresença é o desafio “any-to-any”, e essa dinâmica não só melhorou as nossas comunicações, como também aumentou os pontos de entrada e os métodos que os hackers usam para entrar. Infelizmente, a maneira de a maioria das empresas lidar com a segurança não evoluiu no mesmo ritmo.

A maior parte das empresas protege as redes ampliadas com tecnologias diferentes que não são capazes de trabalhar em conjunto. Elas também podem depender muito de provedores de serviço para conseguir segurança na nuvem e de empresas de hospedagem para proteger a infraestrutura da Internet. Nessa nova realidade, os administradores de segurança muitas vezes têm pouca visibilidade ou controle sobre os dispositivos e aplicativos que acessam a rede corporativa e capacidade limitada para acompanhar as novas ameaças.

Nova dinâmica da segurança

Diante da combinação de ataques avançados e infraestrutura "any-to-any", os profissionais de segurança desejam saber a resposta para três perguntas importantes:

1. *Com os novos modelos de negócios e vetores de ataque, como nós mantemos a segurança e a conformidade à medida que o cenário de TI continua mudando?* As empresas que migram para a nuvem, a virtualização ou dispositivos remotos por causa da produtividade, agilidade e eficiência proporcionadas por essas tecnologias devem alinhar sua infraestrutura de segurança de acordo.
2. *Em um cenário de ameaça em desenvolvimento, como nós melhoramos a capacidade de proteção contínua contra novos vetores de ataque e ameaças cada vez mais sofisticadas?* Os invasores não fazem distinção; eles aproveitarão qualquer brecha na corrente. Eles difundem seus ataques de forma implacável, usando geralmente ferramentas desenvolvidas especificamente para driblar a infraestrutura de segurança escolhida do alvo. Eles fazem todo o possível para não serem detectados, usando tecnologias e métodos que geram indicações de comprometimento praticamente imperceptíveis.
3. *Como vamos responder as primeiras duas perguntas e diminuir a complexidade e a fragmentação das soluções de segurança ao mesmo tempo?* As empresas não podem se dar ao luxo de deixar lacunas na proteção que os hackers sofisticados de hoje exploram. Ao mesmo tempo, adicionar complexidade nas soluções de segurança distintas que não estão integradas não proporcionará o nível de proteção necessário contra ameaças avançadas.

> *"Todas as empresas têm conexões com domínios que são sites de ameaça de malware conhecidos."*
>
> –Relatório de segurança anual da Cisco de 2014

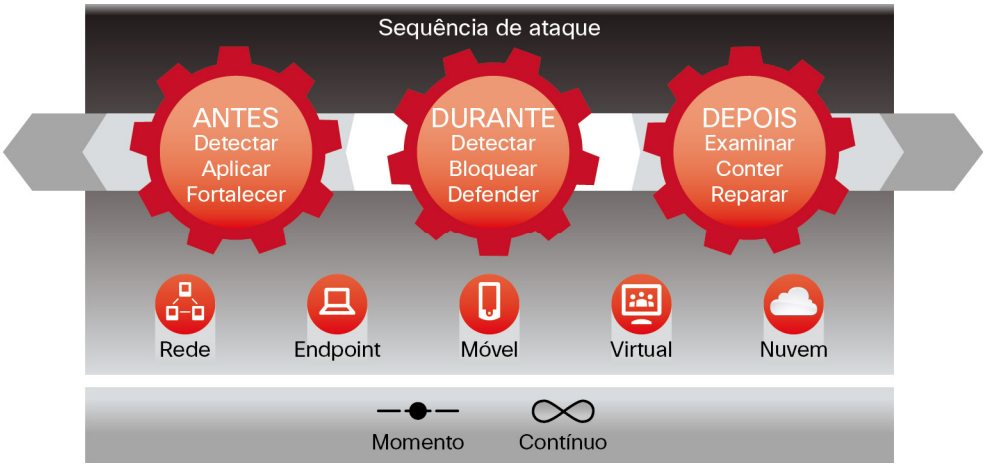
A combinação dessa dinâmica (modelos de negócios em mudança, um cenário de ameaça em desenvolvimento e a complexidade e fragmentação da segurança) tem criado brechas na segurança, interrompido o ciclo de vida da segurança, reduzido a visibilidade e introduzido desafios no gerenciamento da segurança. Para realmente proteger as empresas diante dessa dinâmica, é necessário mudar nossa abordagem de segurança. É hora de termos um novo modelo de segurança centrado na ameaça.

Como lidar com a sequência de ataque completa: antes, durante e depois de um ataque

Atualmente, a maioria das ferramentas de segurança concentra-se em apresentar visibilidade na rede e bloquear o malware no ponto de entrada. Essas tecnologias examinam os arquivos uma vez, em um momento inicial, para determinar se são mal-intencionados. Mas os ataques avançados não acontecem em apenas um momento, eles são contínuos e exigem análise constante. Agora, os adversários empregam táticas como salto de porta, encapsulamento, ataques de dia zero, evasão de detecção de comando e controle (C&C), técnicas de sono, movimento lateral, tráfego criptografado, ameaças combinadas e evasão da sandbox para fugir da detecção inicial. Se o arquivo não for capturado ou se evoluir e se tornar mal-intencionado depois de entrar no ambiente, as tecnologias de detecção pontuais não serão mais úteis para identificar as atividades subsequentes reveladas do invasor.

Os métodos de segurança não podem se concentrar apenas na detecção, mas também devem ser capazes de atenuar o impacto depois da entrada do invasor. As empresas precisam enxergar seu modelo de segurança de forma global e obter visibilidade e controle na rede ampliada e na sequência de ataque completa: antes de um ataque ocorrer, durante e até mesmo depois de ele começar a prejudicar os sistemas e roubar informações (consulte a Figura 2).

Figura 2. O novo modelo de segurança



- **Antes:** os defensores precisam de amplo conhecimento e visibilidade sobre o que está na rede ampliada para implementar as políticas e os controles que a defenderão.
- **Durante:** a capacidade de detectar malware e bloqueá-lo de forma contínua é essencial.
- **Depois:** os defensores precisam da segurança retrospectiva para marginalizar o impacto de um ataque. Eles devem identificar o ponto de entrada, determinar o escopo, conter a ameaça, eliminar o risco de uma nova infecção e solucionar o transtorno.

Antes de um ataque

Invasores contextuais exigem uma segurança contextual. As empresas lutam contra invasores que têm mais informações sobre a infraestrutura do que os próprios defensores que tentam protegê-la. Para se defender antes de ocorrer um ataque, as empresas precisam de total visibilidade do seu ambiente (incluindo, entre outros, hosts físicos e virtuais, sistemas operacionais, aplicativos, serviços, protocolos, usuários, conteúdo e comportamento da rede) na esperança de conseguir mais informações do que os invasores. Os defensores precisam entender os riscos da sua infraestrutura, com base no valor do seu alvo, na legitimidade de um ataque e no histórico. Se eles não souberem o que estão tentando proteger, não estarão preparados para configurar a defesa das tecnologias de segurança. A visibilidade precisa abranger toda a rede: endpoints, gateways de e-mail e da Web, ambientes virtuais, dispositivos móveis e o data center. Além disso, alertas acionáveis devem ser gerados a partir dessa visibilidade para que os defensores possam tomar decisões com base em informações.

Durante um ataque

Ataques severos não ocorrem apenas de maneira pontual. Eles são uma atividade contínua e exigem segurança constante. As tecnologias tradicionais de segurança podem detectar um ataque apenas em um momento, com base em um único ponto de dados do próprio ataque. Essa abordagem não consegue combater ataques avançados. Em vez disso, é necessário haver uma infraestrutura de segurança com base no conceito de reconhecimento; uma que possa agregar e correlacionar os dados da rede ampliada aos padrões antigos e à inteligência de ataque global para oferecer contexto e diferenciar ataques ativos, extração e reconhecimento em relação ao simples ruído de fundo. Isso faz a segurança evoluir de um exercício pontual para uma análise e tomada de decisão contínua. Se um arquivo for considerado seguro, mas depois demonstrar um comportamento mal-intencionado, as empresas poderão agir. Com essa segurança de visão em tempo real, os profissionais poderão empregar a automação inteligente para aplicar políticas de segurança sem intervenção manual.

Depois de um ataque

Para lidar com a sequência de ataque completa, as empresas precisam da segurança retrospectiva. A segurança retrospectiva é um desafio de big data e um recurso que poucos podem oferecer. Com uma infraestrutura que pode coletar e analisar dados continuamente para criar inteligência de segurança, as equipes de segurança podem, com a automação, identificar indicações de comprometimento, detectar malware que seja sofisticado o suficiente para alterar o seu comportamento evitando a detecção e, então, solucionar o problema. Comprometimentos que não seriam detectados por semanas ou meses podem ser identificados, definidos e corrigidos.

Esse modelo de segurança centrado na ameaça permite que as empresas lidem com a sequência de ataque completa, em todos os vetores de ataque e reajam a qualquer momento, a todo o momento e em tempo real.

Como ativar o novo modelo de segurança

Para ativar o novo modelo de segurança, a Cisco acredita que as tecnologias modernas de segurança precisam se concentrar em três obrigações estratégicas: devem estar orientadas pela visibilidade, concentradas na ameaça e baseadas no desempenho.

Orientadas pela visibilidade: Os administradores de segurança devem ser capazes de visualizar com exatidão tudo o que está acontecendo. Essa capacidade requer uma combinação de largura e profundidade (consulte a Figura 3). Largura é ter a capacidade de visualizar e coletar dados de todos os possíveis vetores de ataque na estrutura da rede, endpoints, gateways de e-mail e da Web, dispositivos móveis, ambientes virtuais e na nuvem para obter o conhecimento sobre os ambientes e as ameaças. A profundidade proporciona a capacidade de correlacionar essas informações, aplicar a inteligência para entender o contexto, tomar decisões melhores e agir de forma manual ou automática.

Figura 3. Largura e profundidade

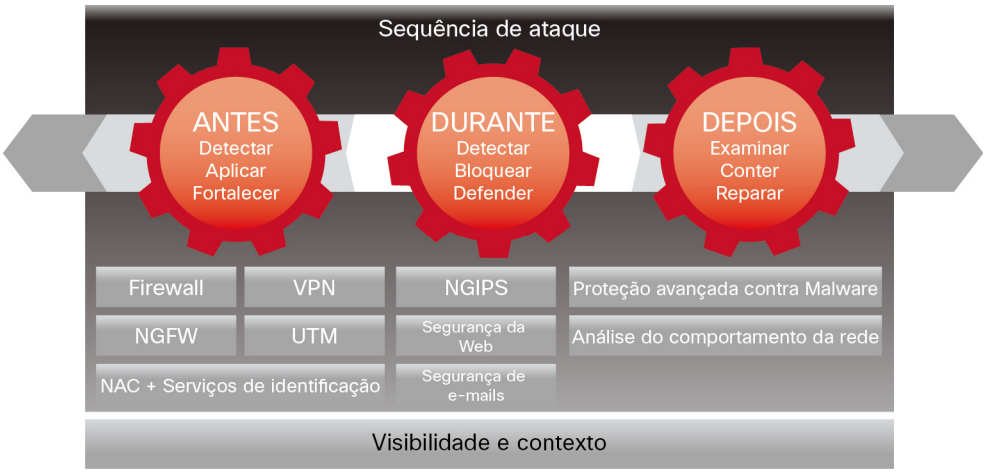
Concentradas na ameaça: As redes atuais alcançam os funcionários onde quer que eles estejam e se estendem aos dados, não importa onde estejam ou de onde possam ser acessados. Apesar dos grandes esforços, acompanhar a constante evolução dos vetores de ataque é um desafio para os profissionais de segurança e uma oportunidade para os invasores. As políticas e controles são fundamentais para diminuir a área de ataque, mas as ameaças ainda existem. Sendo assim, as tecnologias também devem se concentrar na detecção, compreensão e interrupção das ameaças. Concentrar-se nas ameaças significa pensar como um invasor, aplicar a visibilidade e o contexto para compreender e adaptar-se às mudanças no ambiente, além de desenvolver proteções para agir e interromper ameaças. Com o malware avançado e ataques de dia zero, esse é um processo contínuo que requer análise constante e inteligência de segurança em tempo real fornecida na nuvem e compartilhada em todos os produtos para melhor eficácia.

Baseada na plataforma: A segurança é agora mais do que um problema da rede; ela exige um sistema integrado de plataformas ágeis e abertas que cobrem a rede, os dispositivos e a nuvem. Essas plataformas precisam ser extensíveis, criadas por escala e gerenciadas de forma central para uma política unificada e controles consistentes. Simplificando: elas precisam estar tão difundidas quanto os ataques que estamos combatendo. Isso representa uma mudança na implantação de dispositivos de segurança de ponto único para integrar uma plataforma real de serviços e aplicativos escaláveis e de fácil implantação. Uma abordagem com base na plataforma não só aumenta a eficácia da segurança, eliminando silos e as brechas da segurança criadas, como também acelera o tempo de detecção e simplifica a aplicação.

Cobertura da sequência de ataque completa

Para vencer os desafios de segurança atuais e conseguir maior proteção, as empresas precisam de soluções que se estendam sobre a sequência de ataque inteira e sejam projetadas com base nos princípios de serem orientadas pela visibilidade, concentradas na ameaça e baseadas na plataforma. A Cisco oferece um portfólio amplo de soluções de segurança cibernética centradas na ameaça que se estendam sobre a sequência de ataque inteira.

Figura 4. Cobertura da sequência de ataque inteira



Essas soluções específicas baseadas na plataforma oferecem o conjunto mais amplo do setor de opções de aplicação e reparo de vetores de ataque em que as ameaças se manifestam. Essas soluções trabalham em conjunto para proporcionar proteção na sequência de ataque e são integradas para tornarem-se soluções complementares para um sistema de segurança geral.

- Antes de um ataque, as soluções que incluem firewalls, firewalls de última geração, controle de acesso à rede e serviços de identificação, entre outros, dão aos profissionais de segurança as ferramentas de que precisam para detectar ameaças, além de aplicar e fortalecer políticas.
- Durante um ataque, os sistemas de prevenção de intrusão de próxima geração (NGIPS, Next-Generation Intrusion Prevention Systems) e as soluções de segurança de e-mail e da Web oferecem a capacidade de detecção, bloqueio e defesa contra ataques que entraram na rede e estão em andamento.
- Depois de um ataque, as empresas podem aproveitar o Cisco Advanced Malware Protection e a análise do comportamento da rede para definir o escopo, conter e reparar com rapidez e eficácia um ataque para minimizar os danos.

Essas soluções são escaláveis para oferecer suporte até mesmo para as maiores empresas do mundo, e por isso estão disponíveis quando e como as empresas precisarem delas, como dispositivos físicos e virtuais, ou como serviços na nuvem. Elas também estão integradas para oferecer visibilidade contínua e controle na rede ampliada e em todos os vetores de ataque.

Conclusão

A industrialização da invasão, junto com o desafio any-to-any, está mudando profundamente a maneira como nós devemos proteger os nossos sistemas, levando-nos a pensar em uma nova abordagem para a segurança cibernética. As estratégias de segurança que se concentram nas defesas baseadas no perímetro e nas técnicas de prevenção apenas deixarão os invasores livres para agir como quiserem quando entrarem na rede.

Os dinâmicos modelos de negócios, um cenário de ameaça em desenvolvimento e a complexidade e fragmentação da segurança têm criado brechas na segurança, interrompido o ciclo de vida da segurança, reduzido a visibilidade e introduzido desafios no gerenciamento da segurança. É hora de um novo modelo de segurança centrado na ameaça que proporcione a visibilidade e o controle de que as empresas precisam na rede ampliada e na sequência de ataque completa.

A Cisco é a única capaz de fornecer uma abordagem centrada na ameaça para a segurança que diminui a complexidade e fornece visibilidade superior, controle contínuo e proteção contra ameaça avançada na sequência de ataque inteira. Com esse novo modelo de segurança, as empresas podem agir com mais inteligência e rapidez antes, durante e depois de um ataque.

Sede - América
Cisco Systems. Inc
San Jose. CA

Sede - Ásia e Pacífico
Cisco Systems (USA) Pad Ltd.
Cingapura

Sede - Europa
Cisco Systems International BV Amsterdam,
Países Baixos

A Cisco possui mais de 200 escritórios no mundo todo. Os endereços, números de telefones e fax estão disponíveis no site **www.cisco.com/go/offices**.

Impresso nos EUA C11-731741-01 06/14