Proteção avançada contra malware:

Guia para compradores

Guia para compradores da proteção avançada contra malware

O que você vai aprender

Este documento vai identificar os recursos essenciais de que você precisa em uma solução de proteção avançada contra malware e as perguntas importantes que você deve perguntar ao fornecedor, além de mostrar como a Cisco combate os ataques de malware avançado atuais com uma combinação de quatro técnicas:

- Dados analíticos avançados
- Inteligência de ameaças de segurança global coletiva
- Aplicação em vários formatos (redes, endpoints, dispositivos móveis, gateways seguros e sistemas virtuais)
- Análise contínua e segurança retrospectiva

Introdução

Não é segredo nenhum que os invasores de hoje têm recursos, conhecimento e persistência para comprometer as operações de qualquer empresa caso não sejam detidos em tempo. As defesas tradicionais, inclusive firewalls e antivírus de endpoint, não funcionam mais contra esses ataques. O modo de lidar com o malware precisa evoluir urgentemente. A detecção de ataques de malware direcionados e persistentes é um problema grande demais para ser solucionado por um único controle pontual ou produto. A proteção avançada contra malware exige um conjunto integrado de controles e um processo contínuo para detectar, confirmar, rastrear, analisar e reparar essas ameaças antes, durante e após os ataques.

Perguntas que você deve fazer ao fornecedor

- Como você usa o big data para identificar malwares persistentes?
- Como o malware é analisado para que sua finalidade seja identificada com precisão?
- Como sua análise de malware atualiza automaticamente as funcionalidades de detecção?
- Como você coleta informações sobre novas ameaças de malware?
- Quais são os processos de análise contínua para detecção de malware já instalado?

O problema vai piorar antes de melhorar. Com o surgimento do malware polimórfico, as empresas enfrentam dezenas de milhares de novos malwares por hora e os invasores precisam de ferramentas relativamente simples para colocar os dispositivos em risco. A criação de listas de bloqueio com base na correspondência entre arquivos e assinaturas de malware conhecidas não consegue mais acompanhar o ritmo das invasões, e as técnicas mais modernas de detecção, como sandboxing, não são 100% eficazes.

Análise avançada e informações coletivas de segurança

Em uma tentativa de atender melhor aos clientes em vista do crescimento exponencial de malwares conhecidos, os fornecedores de proteção tradicional para endpoints disponibilizaram um "antivírus com auxílio da nuvem" que basicamente migrava os bancos de dados de assinaturas para a nuvem. Essa medida solucionou a necessidade de distribuir bilhões de assinaturas de vírus a cada endpoint a cada cinco minutos, mas não interrompeu a evolução de malwares avançados criados para despistar a detecção com base em assinaturas.

Com o desenvolvimento de malwares que agem pacientemente, os invasores exploraram outra limitação do modelo de antivírus auxiliado pela nuvem: a maioria das tecnologias antimalware não é persistente e não leva o contexto em consideração. Elas se concentram somente na detecção quando o arquivo é identificado pela primeira vez (detecção pontual). No entanto, o que hoje é inofensivo pode facilmente tornar-se mal-intencionado amanhã. A verdadeira proteção só pode ser alcançada através da análise contínua. O monitoramento constante de todo o tráfego ajuda a equipe de segurança a verificar a origem de uma infecção quando a disposição de um arquivo muda.

Os criadores de malware avançado usam diversas técnicas para ocultar a intenção do malware e dificultar a sua detecção. Dentre essas inovações estão os arquivos polimórficos, que mudam para enganar os mecanismos de assinaturas, programas de download sofisticados que obtêm malware sob demanda de redes CnC (command-and-control, comando e controle) e Trojans obliteráveis que excluem seus próprios componentes, o que dificulta a localização do malware e a análise feita pelos investigadores. Esses são apenas alguns exemplos.

Como o malware já não pode ser identificado por sua "aparência", uma defesa eficaz precisa de novas técnicas para capturar e analisar o malware ao longo do seu ciclo de vida. Esse novo modelo de informações de segurança proativa gera uma compreensão do que o malware faz e para onde ele vai. As ameaças de hoje em dia podem driblar as defesas que implantam estratégias pontuais ao executar e indicar o comprometimento de um sistema muito depois do período de detecção inicial.

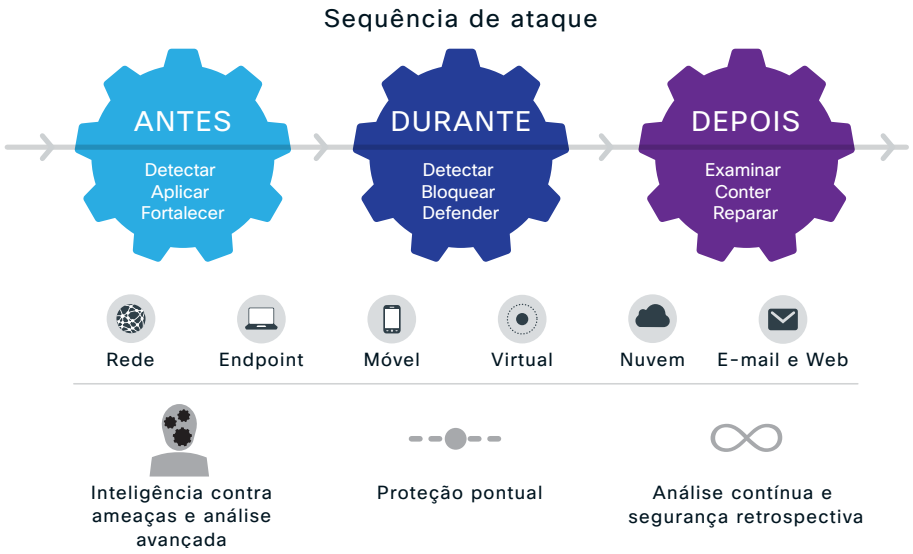
Sua abordagem ao malware deve adaptar-se tão rapidamente quanto a ameaça. A Cisco adotou uma nova abordagem mais ampla para lidar com os desafios da detecção de malware. Com o apoio de uma base global composta por milhares de empresas e milhões de endpoints, coletamos todos os meses milhões de amostras de malware. Nossos mecanismos de análise do Threat Grid, o Cisco Talos Security Intelligence and Research Group (Talos) e nossa nuvem de Collective Security Intelligence (CSI) analisam dezenas de milhares de atributos de software para separar o malware do software benigno. Também analisamos as características do tráfego de rede para identificar malware que procura redes CnC. Usamos nossa ampla base de instalações de proteção contra malware avançado (AMP) em nossas linhas de produtos[1] para verificar a aparência dos arquivos e da atividade de rede normais, globalmente e nas empresas de clientes específicos para fins de comparação.

1. Os recursos da AMP agora estão disponíveis como um recurso com licença adicional nas soluções de segurança da Web e de e-mail da Cisco. Para obter mais informações, acesse http://www.cisco.com/go/amp.

A detecção de malware projetado para driblar as táticas tradicionais de detecção exige ainda mais sofisticação. A Cisco usa modelos concebidos especialmente para identificar malware com base em suas ações, e não em sua aparência. Dessa forma, é possível detectar novos tipos de ataques, até mesmo os de dia zero. Para acompanhar o ritmo das mudanças de malware, esses modelos são atualizados automaticamente em tempo real com métodos de ataques descobertos pelos mecanismos de análise do Threat Grid e pelo Talos Security Intelligence and Research Group.

A integração da tecnologia do Threat Grid à AMP também oferece inteligência de ameaças adicional e mecanismos de análise de malware estáticos e dinâmicos (sandboxing). Agora integrado à AMP, o Threat Grid (também disponível como solução independente) oferece às equipes de segurança uma base de conhecimento de malware adicional proveniente do mundo todo. As empresas obtêm feeds ricos em contexto disponibilizados em formatos padrão para integrar-se com perfeição às tecnologias de segurança atuais; a análise de milhões de amostras todos os meses em relação a mais de 350 indicadores de comportamento, que resulta em bilhões de artefatos e uma pontuação de ameaças de fácil entendimento para ajudar as equipes de segurança a priorizar as ameaças. Os mecanismos de análise do Threat Grid identificam o que o malware está fazendo, inclusive o tráfego HTTP e DNS associados, os fluxos TCP/IP, os processos que ele está afetando e a atividade de registro, o que permite que as equipes de segurança se informem melhor sobre as possíveis ameaças em suas redes.

Figura 1. A abordagem de segurança da Cisco oferece proteção antes, durante e depois de um ataque, em vários vetores de ataque, além de oferecer análise contínua e segurança retrospectiva, bem como técnicas tradicionais de detecção pontual.



Outros benefícios englobam a análise de nuvem que avalia arquivos durante um período prolongado. As soluções da AMP podem emitir alertas muito além da primeira vez que o arquivo é analisado, mesmo que ele tenha passado por um ponto de detecção.

Por fim, esses benefícios se estendem a toda a comunidade da Cisco AMP. A AMP envia um alerta sempre que a disposição de um arquivo muda. Nesse caso, todas as empresas que usam a Cisco AMP são imediatamente alertadas sobre o arquivo mal-intencionado, o que possibilita a "imunidade coletiva" viabilizada pelo potencial da nuvem.

A segurança retrospectiva volta ao momento anterior aos ataques

Os invasores estão sempre ativos. Eles sempre avaliam os controles de segurança usados e mudam suas táticas para ficar um passo à frente das defesas. Na verdade, a maioria dos invasores testa os malwares em produtos antimalware líderes de mercado antes de lançar os ataques. À medida que a eficiência das listas de bloqueio diminuem, cada vez mais as empresas de segurança utilizam análises dinâmicas em máquina virtual (VM) para expor e estudar o malware. Em resposta, os invasores adaptaram suas táticas: eles não fazem nada ou atrasam a execução do ataque em arquivos que passam por essa VM por algumas horas (ou dias). Eles presumem que o arquivo escapará da detecção por não ter feito nada mal-intencionado durante o período de avaliação. Obviamente, após esse período de espera, o malware compromete o dispositivo.

Infelizmente, as tecnologias pontuais não podem analisar um arquivo novamente. Quando um arquivo é considerado seguro, ele permanece com esse status, independentemente das melhorias nas técnicas de detecção ou da apresentação de características de malware. E o que é ainda pior: depois que o malware despista a detecção, esses controles não conseguem rastrear sua propagação no ambiente, verificar as causas iniciais nem identificar os possíveis gateways do malware (sistemas que são infectados pelo malware diversas vezes ou que funcionam como plataforma de lançamento para infecções mais extensas).

Segurança retrospectiva

O uso de análise contínua para constantemente investigar o comportamento de arquivos, rastrear processos, atividades de arquivos e comunicações no decorrer do tempo, para compreender a amplitude real da infecção, determinar as causas iniciais e realizar a correção. Isso permite voltar no tempo e impedir possíveis ataques. A segurança retrospectiva é necessária quando há indicadores de comprometimento, como um iniciador de eventos, uma alteração na disposição de um arquivo ou um iniciador de IoC (Indication of Compromise, Indicador de comprometimento).

A melhor abordagem é supor que nenhuma medida de detecção será 100% eficaz. Acreditar que essas medidas proporcionarão proteção total superestima sua capacidade em defender recursos básicos e subestima a capacidade dos adversários em atacá-los. As empresas devem presumir que suas defesas serão dribladas. Elas devem conseguir identificar o escopo e o contexto das infecções, conter os danos com rapidez e eliminar a ameaça, as causas iniciais e os gateways do malware. Esse recurso exige segurança retrospectiva.

Nossa tecnologia de segurança retrospectiva permite voltar no tempo e verificar quais dispositivos foram expostos a um malware, independentemente do momento em que o arquivo comprometido é identificado. Dois atributos oferecem esse recurso: trajetória do arquivo e indicadores de comprometimento (CPI). A trajetória do arquivo rastreia cada arquivo que atravessa a rede protegida e oferece acesso a um histórico completo das ações de cada dispositivo protegido que foi exposto. Os IoCs usam as informações da trajetória do arquivo para criar um padrão de comportamento que pode ser usado para descobrir se há algum malware no sistema que não tenha sido detectado.

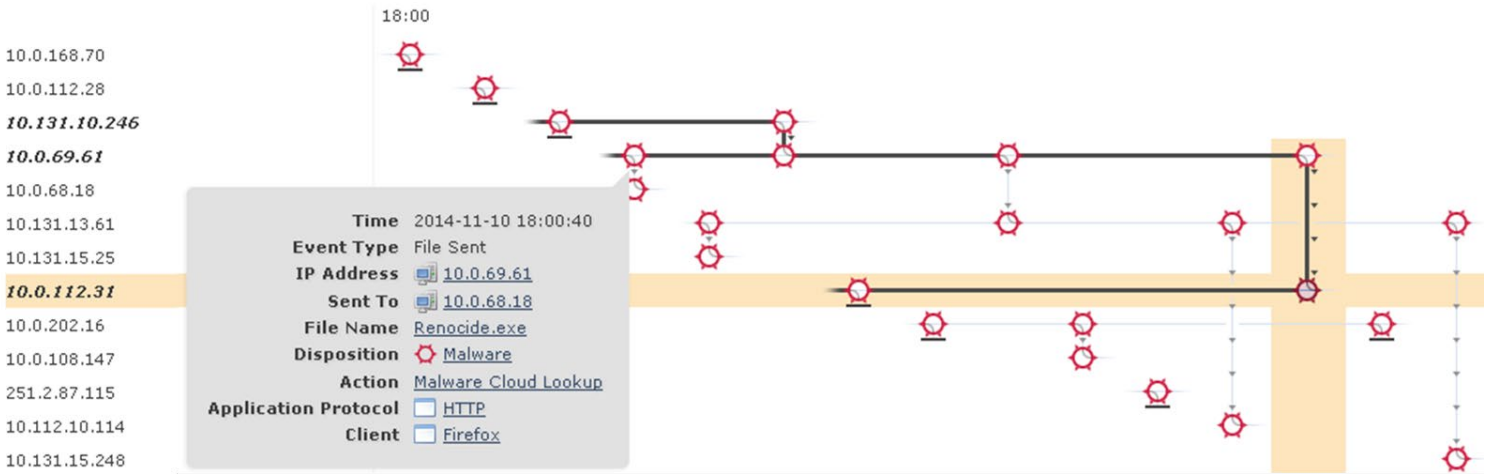
Rastreamento de malware através da trajetória

Se em algum momento no futuro um arquivo provar ser um malware, você terá opções limitadas com as defesas antimalware tradicionais. Não é possível usar uma máquina do tempo e bloquear o arquivo no momento de sua entrada. Ele já está no ambiente, e você não tem ideia do quanto ele já se disseminou ou o que ele já fez. É nesse momento que a maioria dos controles antimalware deixa você às cegas quanto ao alcance do problema e sem capacidade de descobri-lo.

Descubra o Big Data e a análise avançada por trás da AMP. Nosso recurso de análise de trajetória verifica com rapidez e precisão como o malware passou pela empresa. Em alguns casos, é possível limpar os dispositivos afetados de maneira imediata e automática. A análise de trajetória apresenta um mapeamento visual da passagem dos arquivos pela empresa e do que eles fizeram no sistema. Mas você não vê apenas a atividade do arquivo pela rede. A AMP também pode mostrar a atividade detalhada de cada executável em um único endpoint, independentemente da disposição do arquivo. A capacidade de desviar sua atenção da atividade em um endpoint para o local onde os arquivos mal-intencionados migraram para outros endpoints através da rede estendida oferece um alto nível de visibilidade para as equipes de segurança. E o que é ainda mais importante: como a AMP rastreia todo o uso do arquivo, você pode identificar o "paciente zero", a primeira vítima do malware, e todos os demais dispositivos infectados, o que ajuda a assegurar a total erradicação da infecção. Todos sabem que se uma única instância do malware resistir à limpeza, os riscos de uma nova infecção permanecem altos.

Além disso, a trajetória não somente analisa informações relacionadas à atividade do arquivo. Ela também pode rastrear informações sobre a linhagem, o uso, as dependências, as comunicações e os protocolos do arquivo. A trajetória pode identificar quais arquivos estão instalando malware a fim de facilitar uma rápida análise da causa original do malware detectado ou da atividade suspeita. As equipes de segurança podem assumir o controle durante o ataque e compreender com rapidez o escopo e suas causas iniciais a fim de impedir a proliferação da infecção com eficiência.

Figura 2. Uma tela de trajetória do arquivo, que mostra a propagação do malware e informações sobre o ponto de entrada, a atividade do malware e os endpoints envolvidos.

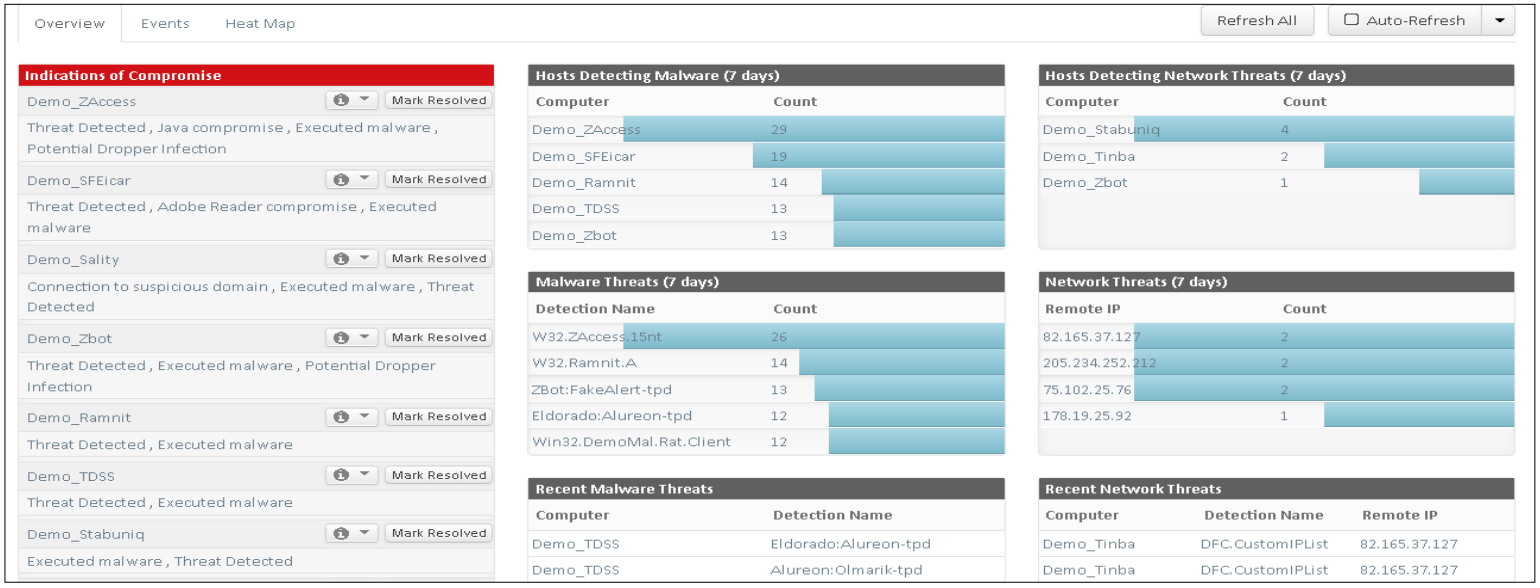


A determinação de qual evento exige priorização e resposta imediata pode ser um grande desafio quando você se depara com um número elevado de eventos de detecção, especialmente quando se trata de malware. Um único evento, mesmo um arquivo mal-intencionado bloqueado em um endpoint, nem sempre implica um comprometimento. Entretanto, quando diversos eventos estão correlacionados, mesmo que se trate de várias atividades aparentemente benignas, o resultado pode aumentar consideravelmente o risco de comprometimento de um sistema. Assim, a violação é iminente ou pode já estar em andamento.

IoCs identificam padrões, não impressões digitais

O recurso Indicadores de Comprometimento (IoC) da AMP permite fazer análises mais detalhadas para localizar sistemas que demonstram sintomas de comprometimento ativo. Esse recurso vai muito além do que as tecnologias de detecção pontuais podem oferecer, pois continua capturando, analisando e correlacionando atividades de malware após a primeira análise, o que possibilita a análise automatizada e priorização de riscos.

Figura 3. Uma tela do painel da Cisco AMP mostrando IoCs em um sistema.



Por fim, depois de estabelecido dentro de uma empresa, o malware geralmente tenta se comunicar com os servidores CnC ou, caso seja controlado diretamente por um invasor, inicia atividades de reconhecimento para mover-se em direção ao alvo.

A Cisco AMP monitora a atividade de comunicação no endpoint protegido e a correlaciona com a inteligência em segurança coletiva para verificar se há um comprometimento e bloquear a comunicação e a distribuição do malware no endpoint. Essa ação oferece uma vantagem única para a equipe de segurança no controle da proliferação do malware nos endpoints que podem não estar incluídos nas proteções da rede corporativa, como os sistemas usados por funcionários remotos ou móveis. Além disso, a trajetória e os IoCs usam a atividade de rede capturada para acelerar as investigações e priorizar as ameaças.

Os esforços conjuntos são melhores: aplicação na rede, no gateway seguro, em endpoints físicos e virtuais e em dispositivos móveis

Nenhum controle de segurança persiste ao vácuo. A defesa contra malware avançado exige uma coordenação considerável entre as defesas de rede, gateway e endpoint. Se você quer aumentar a velocidade de detecção e resposta e deter invasões de malware antes que elas se materializem em violações de alto nível, suas ferramentas de segurança precisam trabalhar em conjunto, compartilhar informações e correlacionar eventos. Também se faz necessário um console de gerenciamento central que controle as ameaças e as atividades de correção em todos os níveis. A Cisco oferece um sistema integrado com informações de segurança em nuvem, análise de rede avançada e diversos pontos de aplicação para ajudar a assegurar que o malware avançado não passe despercebido em sua empresa.

Os amplos recursos da AMP iniciam a proteção na rede para detectar e bloquear o malware conforme ele se desloca. Assim que cada arquivo entra ou sai da rede, a AMP para redes gera uma impressão digital para o arquivo e consulta o Centro de gerenciamento do Cisco FireSIGHT™ a fim de verificar se o arquivo foi identificado como mal-intencionado.

Se o Centro de gerenciamento não reconhecer o arquivo, ele consultará as informações de segurança coletiva e verificará se há registros desse arquivo em nossa rede de informações de segurança. Essa busca superficial é uma abordagem mais escalável e não tem impacto na latência do sistema (diferente do sandboxing de cada arquivo da rede). Quando um arquivo é identificado como mal-intencionado, o Centro de gerenciamento aplica os recursos da análise de trajetória do arquivo para compreender o contexto e a extensão da exposição.

Também é possível implementar o agente de proteção superficial contra malware da Cisco destinado a endpoints, o conector AMP™, em cada dispositivo protegido para que todas as atividades do arquivo possam ser verificadas em relação às informações de segurança coletiva e no malware conhecido. A AMP para endpoints não procura apenas arquivos mal-intencionados, mas também detecta e bloqueia o comportamento de malware em dispositivos protegidos. Mesmo que não haja registros do arquivo, os endpoints são protegidos contra ataque de dia zero. A AMP para endpoints também utiliza os recursos de segurança retrospectiva e de trajetória do arquivo descritas anteriormente para identificar a extensão de qualquer ataque e identificar quais dispositivos precisam de reparos imediatos.

Se o arquivo for sinalizado como suspeito, a AMP fará uma análise mais detalhada. Conforme descrito anteriormente, a análise da Cisco em nuvem verifica exatamente o que o arquivo faz e analisa o ataque caso ele seja categorizado como malware. A tecnologia agora está integrada à AMP para endpoints, trazendo feeds de inteligência adicionais e mecanismos de análise estática e análise dinâmica para investigar o malware de maneira ainda mais detalhada. Esse processo gera IoCs que podem ser usados para localizar o malware que pode já estar na rede.

Com esses perfis de malware, a AMP capacita as empresas para tomarem medidas proativas contra ataques de malware. Se um arquivo for categorizado como malicioso após o fato (usando a segurança retrospectiva) ou se for identificado em outro ambiente da comunidade da Cisco AMP, o CSI Cloud enviará as informações atualizadas para o centro de gerenciamento em sua empresa para que você possa bloquear o malware na rede ou no endpoint. Ao fazer isso, você obtém imunidade coletiva com o restante da comunidade da Cisco AMP. Além disso, você pode definir regras personalizadas para bloquear arquivos e endereços IP específicos se os administradores locais identificarem um ataque localizado que precise de ação imediata.

A Cisco AMP para endpoints também protege dispositivos móveis. O conector móvel da AMP tem como base essa mesma nuvem de informações de segurança para analisar aplicativos Android com rapidez, em busca de possíveis ameaças em tempo real. Com a expansão da visibilidade para dispositivos móveis, você pode descobrir rapidamente quais dispositivos estão infectados e quais aplicativos estão introduzindo o malware no sistema. Você pode reparar o ataque com controles eficientes para criar uma lista de bloqueios para aplicativos específicos, a fim de indicar quais aplicativos poderão ser usados nos dispositivos móveis que acessarem os recursos da empresa.

Agora, os recursos da AMP também estão disponíveis em gateways de segurança da Web e de e-mail da Cisco, no Cisco Cloud Web Security e no Cisco ASA com FirePOWER Services. Com os recursos da AMP agregados a esses dispositivos, é possível melhorar a detecção e bloquear o malware avançado nos possíveis pontos de entrada. Dentre os recursos da AMP estão a reputação e o sandboxing de arquivos conforme descrito acima. Além disso, os alertas retrospectivos proporcionam a análise contínua dos arquivos que transitam pelos gateways, com o uso de atualizações em tempo real do CSI Cloud para ficar a par das constantes mudanças nos níveis das ameaças. Assim que um arquivo mal-intencionado é identificado como uma ameaça, os administradores são alertados pela AMP e podem saber quais áreas e aplicativos na rede podem ter sido infectados e quando. Por isso, os clientes conseguem identificar e lidar com um ataque rapidamente, antes que ele tenha a chance de se espalhar.

Conforme explicado anteriormente, o malware pode se infiltrar na empresa através de vários vetores de ataque. Portanto, é essencial ter visibilidade sobre as atividades em toda a empresa. Com o aproveitamento de nossa rede de informações de segurança global e de um recurso para detectar, bloquear, rastrear, investigar e remediar ataques no gateway, na rede, nos endpoints, em dispositivos móveis e em sistemas virtuais, as empresas podem eliminar pontos cegos inerentes a outros controles de segurança que não têm uma ampla cobertura.

Para obter uma lista completa das implantações da AMP e de seus recursos, acesse http://www.cisco.com/go/amp

AMP em Ação

Um exemplo real é normalmente a melhor maneira de testemunhar o potencial de uma solução integrada de proteção avançada contra malware. A AMP trabalhou para detectar um ataque de dia zero no Java 48 horas antes de ele ser anunciado publicamente. Nesse exemplo, a AMP para endpoints detectou um comportamento estranho em vários dispositivos. O cliente analisou os arquivos usando o CSI Cloud e constatou que o arquivo era de fato malware.

A etapa seguinte era investigar a extensão do ataque e eliminar a infecção o mais rápido o possível. Para isso, o cliente usou o recurso de análise de trajetória, a fim de descobrir quais dispositivos haviam sido expostos aos arquivos comprometidos ou apresentavam os padrões comportamentais do ataque. Após a limpeza dos dispositivos afetados, o cliente estabeleceu regras personalizadas para bloquear os arquivos, bem como os IoCs.

Mas essas regras personalizadas eram necessárias apenas por um curto período. Após o evento, todos os clientes da AMP receberam o perfil do malware, protegendo-se daquele ataque específico. Como os arquivos e os indicadores foram adicionados ao mecanismo de análise de Big Data, cada ocorrência do ataque foi bloqueada antes de ter a chance de entrar no dispositivo ou na rede. Esse processo também alertou os clientes sobre o ataque, permitindo que eles inspecionassem seus próprios ambientes em busca da ameaça. Assim, uma única ação resultou na proteção global de toda a base de clientes da Cisco AMP, antes mesmo de uma divulgação pública do ataque de dia zero.

Conclusão

Embora o setor reconheça que precisa de soluções inovadoras para detectar e reparar ataques avançados de malware, muitas empresas concentram seus esforços na detecção, seja com pacotes tradicionais de detecção para endpoints ou com defesas "infalíveis". Esse caminho segue em direção ao fracasso, pois o setor continua a se deparar com manchetes sobre perda de dados e violações.

Para conseguir defender-se com eficiência contra ataques modernos, a solução deve lançar mão de análise contínua e análise de Big Data para rastrear a interação dos arquivos e as atividades em toda a rede, em ambientes físicos e virtuais, em endpoints protegidos e em dispositivos móveis. Como muitos ataques permanecem inativos durante o período de detecção tradicional, com a funcionalidade de voltar e alterar a classificação de um arquivo para mal-intencionado e rastrear a trajetória desses arquivos e indicadores pela empresa, é possível conter e reparar com eficiência os danos desses ataques avançados.

Por fim, a proteção avançada contra malware deve ser importante não só para dispositivos de endpoint, como também para redes, dispositivos móveis e sistemas virtuais, a fim de oferecer um nível de proteção difundido e constante, uma vez que não é possível prever o alvo do próximo ataque.

A AMP oferece:

- Flexibilidade na implantação, com uma política constante em endpoints, redes, dispositivos móveis, gateways seguros e sistemas virtuais
- CSI Cloud, que ajuda a identificar e analisar novos ataques antes mesmo que o setor os descubra
- A capacidade de identificar malwares através de retrospectivas e da trajetória, localizar todas as instâncias do malware em questão em sua empresa antes que ele se espalhe
- Imunidade coletiva viabilizada pela comunidade global da Cisco AMP, que acessa a pesquisa do Talos e das amostras de arquivo vistas por milhões de agentes de proteção da AMP

Para incluir soluções da Cisco AMP em sua avaliação de segurança, acesse http://www.cisco.com/go/amp.