SOPHOS
Cybersecurity delivered.

Introdução à caça a ameaças

Guia prático de preparação para procurar e neutralizar ameaças cibernéticas evasivas

Os ataques cibernéticos não param de evoluir. Os adversários utilizam métodos cada vez mais sofisticados e altamente evasivos para facilitar e executar seus ataques. Praticar a caça a atividades mal-intencionadas e neutralizá-las se tornou fator crítico na luta contra as ameaças avançadas – mas não é uma tarefa fácil.

Neste relatório, oferecemos diretrizes para você dar seus primeiros passos na caça a ameaças e um resumo das ferramentas e estruturas que as equipes de segurança podem usar como base para ajudá-las a se manterem à frente das ameaças cibernéticas recentes e responderem rapidamente a possíveis ataques. Também descrevemos os cinco passos que os profissionais de TI devem seguir para se prepararem para a caçada.

Documento técnico Sophos. Agosto, 2022

O estado das ameaças cibernéticas em 2022

Os ataques aumentaram em volume, complexidade e impacto

O desafio que as organizações enfrentam com a segurança cibernética continua a crescer. No último ano, 57% das organizações registraram um aumento no volume de ataques cibernéticos, 59% perceberam o aumento na complexidade dos ataques e 53% disseram que o impacto dos ataques aumentou. Quase três em cada quatro (72%) observaram um aumento em pelo menos uma dessas áreas.

Uma tendência crescente é o aumento em ataques à cadeia de suprimentos, como revelou o incidente com a SolarWinds em março de 2021. Os invasores inseriram instruções modificadas no código-fonte da solução Orion usada pela SolarWinds para gerenciar redes complexas remotamente. Esse backdoor permitiu que os adversários acessassem as redes dos clientes da SolarWinds, incluindo várias agências governamentais.

Ransomware é uma ameaça real para todas as organizações

66% das organizações foram atingidas por ransomwares no ano passado, superior aos 37% em 2020. Trata-se de um aumento de 78% no decorrer de um ano, demonstrando que os adversários estão consideravelmente mais capacitados a executar ataques em escala.

O uso crescente de ferramentas legítimas nos ataques cibernéticos

Os adversários se aproveitam cada vez mais de bootlegs ou cópias piratas de softwares comerciais e ferramentas gratuitas de código aberto. Tipicamente, essas ferramentas são projetadas para simular ataques cibernéticos para melhorar a segurança, mas podem ser exploradas pelos criminosos para trabalharem a favor deles.

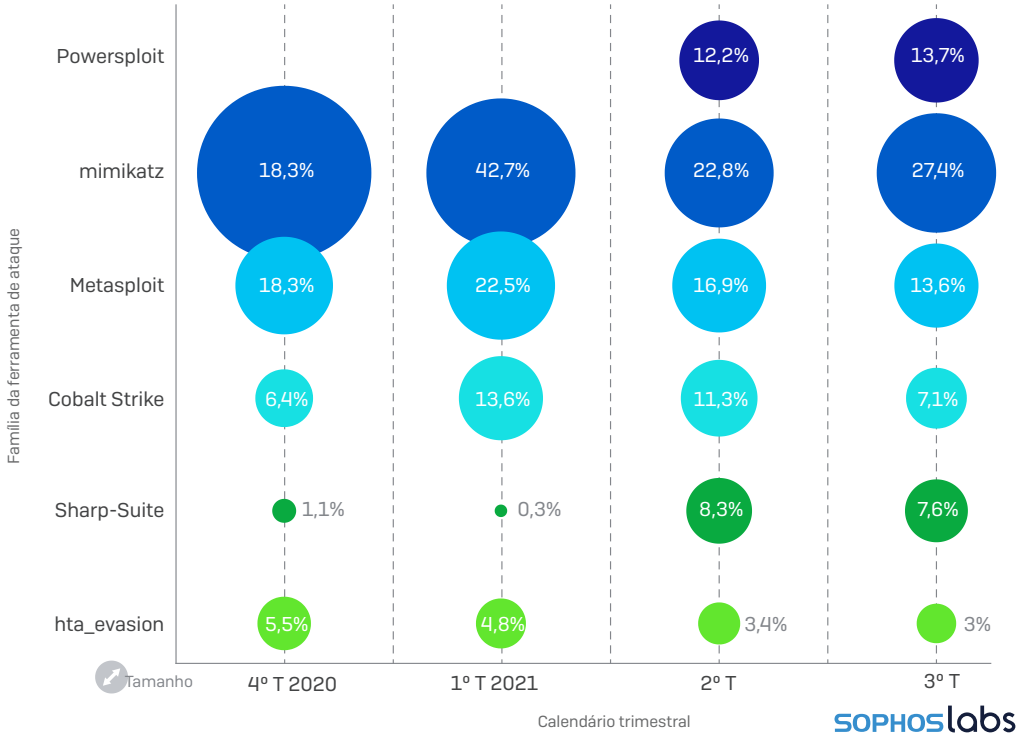
Ferramentas como Mimikatz (usada em pen-tests e por criadores de malwares), ainda que não sejam ferramentas estritamente comerciais, foram bastante usadas, presentes em praticamente todos os incidentes via teclado que a Sophos investigou no decorrer do último ano.

Notoriamente dominantes (graças ao vazamento de seu código-fonte em 2020) também foram as cópias piratas do Cobalt Strike (um software de simulação de adversidades), que não foram usadas apenas em ataques de ransomware, mas também lançadas como carga inicial de outros malwares.

[1] *O Estado do Ransomware 2022 – Sophos*
[2] *O Estado do Ransomware 2022 – Sophos*

Predominância das principais ferramentas de ataque

Em uma análise por máquina, as ferramentas de ataque encontradas com mais frequência observadas em 2020-2021



Relatório de Ameaças 2022 da Sophos

O recurso de "beacons" do Cobalt Strike, que fornece um backdoor apto em computadores Windows, fez desse software uma ferramenta que caiu na preferência dos criminosos cibernéticos. Consequentemente, a maioria dos casos de ransomware observados no ano passado envolveu o uso de Cobalt Strike Beacons.

Para ter uma visão mais detalhada do estado atual das ameaças cibernéticas, acesse o Relatório de Ameaças da Sophos mais recente.

Práticas de segurança cibernética proativas são indispensáveis

Ataques à cadeia de suprimentos. Exploits de software. Ferramentas legítimas. O ponto comum aqui é a natureza dessas abordagens. Elas são comandadas por humanos. Elas são altamente direcionadas e calculadas. Elas são evasivas e indetectáveis pelos meios convencionais.

As organizações devem mudar para abordagens de segurança cibernética mais proativas para se manterem à frente dos criminosos. A resposta a adversários humanos requer uma abordagem comandada por humanos.

Entre na caça a ameaças.

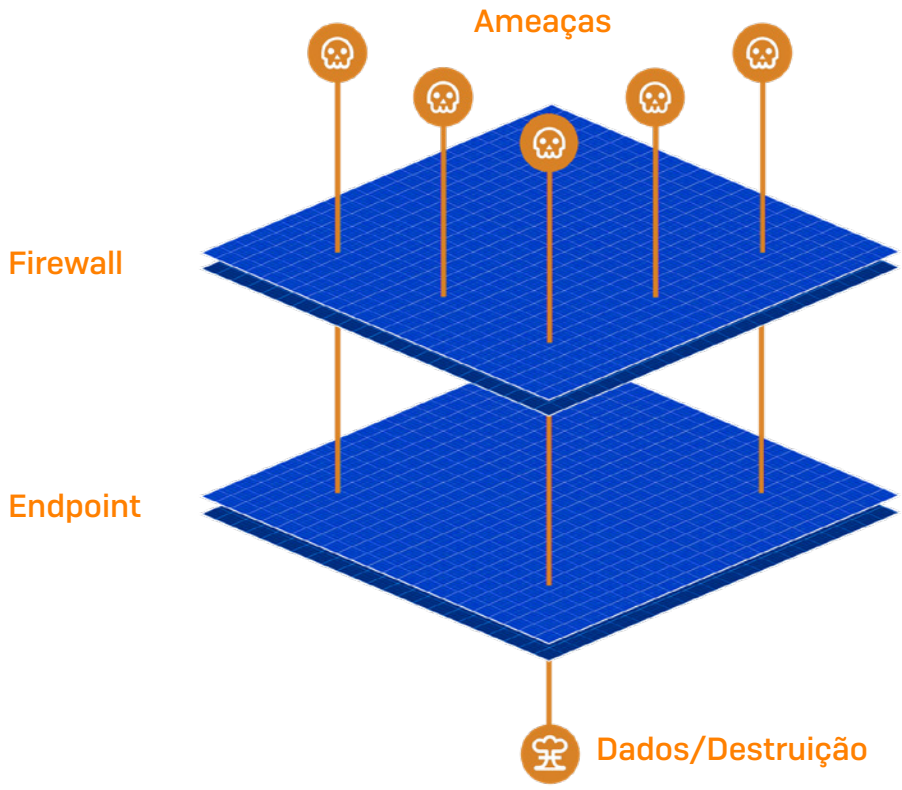
O que é caça a ameaças?

A caça a ameaças é um processo iterativo e proativo de busca por meio da telemetria de endpoints e redes para identificar atividades mal-intencionadas, partindo do pressuposto de que os adversários já burlaram suas defesas. Chamamos isso de iterativo, pois a prática precisa ser adaptada constantemente para garantir que se mantenha um método eficaz de busca e neutralização das ameaças cibernéticas evoluídas de hoje.

Durante a caça a ameaças, as equipes analisam as ferramentas, técnicas e procedimentos (TTPs) usados pelos agentes de ameaças para determinar o estágio do ataque e a inteligência adquirida. Uma vez estabelecidos, as equipes tomam as ações apropriadas para neutralizar a ameaça, se necessário.

Por que precisamos sair no encalço das ameaças?

Os motivos são muitos, mas a razão principal se baseia em uma única verdade: contrário ao que muitos afirmam por aí, a tecnologia sozinha não é capaz de deter 100% das ameaças. Apesar das várias camadas de defesa, algumas ameaças dão um jeito de se infiltrar sorrateiramente e comprometer o seu patrimônio tecnológico.



Como já mencionamos, os agentes de ameaças modernas estão se voltando a abordagens adaptáveis e evasivas em que eles, literalmente, "põem a mão no teclado", em lugar de automatizar e escalar os ataques do passado.

Isso se mostra nas descobertas reveladas por nossas equipes de resposta a ameaças, que relataram um aumento significativo no número de adversários humanos controlando e direcionando ataques. Isso significa que as equipes de segurança precisam sair em busca do desconhecido e incorporar a ideia de que a violação já ocorreu para se manterem um passo à frente nessa corrida.

A mentalidade do caçador de ameaças

Os caçadores mais experientes geralmente consideram que uma ameaça já terá dissipado suas defesas, independentemente de onde ela se encontre na cadeia de ataque. Eles adotam essa mentalidade porque isso os leva a dois pontos de ação.

Limitar o tempo de permanência do agente de ameaça

Adotar essa forma de ação leva as equipes a limitarem o tempo de permanência de um agente. Quanto mais tempo o agente permanecer na rede, mais tempo terá para executar atividades nefastas. Portanto, quanto menos tempo o adversário ficar dentro da sua rede, menos danos poderá causar. Seguindo esse princípio, as equipes de segurança são levadas a sair no encalço de ameaças antes que seu impacto possa ser sentido, pressupondo que suas defesas já tenham sido burladas.

Reduzir o tempo de detecção

Adotar essa mentalidade também leva as equipes a reduzirem o tempo médio de detecção. Você pode ter várias camadas de defesa em operação, e a ameaça pode disparar suas defesas bem mais adiante na cadeia de ataque. O problema é que, quando chega a esse estágio, já é tarde demais: o dano já está feito e a ameaça já atingiu altos patamares. Quando saímos no encalço de uma ameaça, isso nos permite tentar identificar pontos fracos em nossa segurança que podem ser tratados imediatamente, reduzindo o tempo para detectar ameaças idênticas ou similares no futuro.

Quem sai no encalço de ameaças?

O perfil de um caçador de ameaças

Antes de nos aprofundarmos no assunto, é essencial que entendamos o papel de um caçador de ameaças. A caça a ameaças é uma operação altamente complexa. As pessoas que trabalham nesse nicho precisam ter um conjunto específico de habilidades. As características típicas de um caçador de ameaças são:

- **Curiosidade e criatividade** – a busca de ameaças pode se comparar a procurar uma agulha no palheiro. Os caçadores de ameaças podem passar dias procurando ameaças, usando inúmeros métodos para trazê-las à tona.
- **Experiência em segurança cibernética** – a caça a ameaças é uma das operações mais avançadas na segurança cibernética. Portanto, experiência anterior no campo de atuação e conhecimentos básicos são essenciais.
- **Conhecimento do panorama de ameaças** – saber discernir as novas tendências em ameaças é essencial para procurar e neutralizar entidades desconhecidas.
- **Mentalidade antagônica** – a habilidade de pensar como um hacker é ponto crítico para combater abordagens comandadas por humanos.
- **Habilidade de escrever tecnicamente** – caçadores de ameaças devem registrar todas as suas descobertas como parte do processo de investigação. Portanto, a habilidade de comunicar essas informações complexas é um fator crítico para acompanhar a caçada do início ao fim.
- **Conhecimento de redes e sistemas operacionais** – conhecimento avançado sobre redes e sistemas é essencial.
- **Experiência com scripts e codificação** – necessária para ajudar os caçadores de ameaças a criar programas, automatizar tarefas, analisar logs e realizar tarefas de análise de dados para auxiliar e avançar as investigações.

Infelizmente, formar essa rara combinação de competências está muito aquém das possibilidades do setor de TI devido à falta de pessoal capacitado, com 54% dos administradores de TI que acreditam que, mesmo com todas as ferramentas à disposição, os ataques cibernéticos agora estão muito avançados para as equipes de TI lidarem com eles por conta própria. Com isso, quando as vagas são preenchidas, podemos ver claramente que a caça a ameaças é comandada por uma destas duas diferentes equipes.

Centro de Operações de Segurança (SOC) interno

Quando as organizações decidem cuidar da caça a ameaças elas mesmas, você encontrará o seu pessoal no SOC. O SOC é uma funcionalidade comercial interna e centralizada com enfoque no monitoramento, detecção, investigação e resposta a ameaças que melhora a postura de segura geral da empresa matriz. Eles são o ponto de contato na organização no que concerne a assuntos de segurança cibernética.

Provedores terceirizados de operações de segurança

Muitas organizações estão passando suas operações de segurança para provedores terceirizados. Isso pode ser devido à falta de capacidade interna (as equipes de TI observaram um aumento de 69% na carga de trabalho em segurança cibernética no último ano), falta de competência técnica ou preferência por peritos externos para essa tarefa diária infindável.

Provedores de detecção e resposta gerenciadas (MDR)

O MDR, um serviço totalmente gerenciado, oferece às organizações uma equipe dedicada de analistas de segurança que saem no encalço de ameaças obscuras 24 horas por dia, sete dias por semana e 365 dias por ano. De fato, e de acordo com a ESG Research, "51% utilizam um provedor de serviço de detecção e resposta gerenciadas (MDR) para ajudar a integrar os dados de telemetria para a detecção e resposta a ameaças".

Os provedores de MDR oferecem várias vantagens em comparação ao programa de operações de segurança apenas. A maior vantagem dentre todas é, geralmente, a experiência.

A equipe do Sophos MDR tem milhares de horas de experiência, já tendo presenciado e lidado com tudo o que os adversários podem lançar contra o seu pessoal. Eles também podem aprender com os ataques contra outras organizações e aplicar esse ensinamento adquirido a todos os outros clientes. Outro benefício é a escala: a equipe do Sophos MDR pode fornecer suporte 24/7 entregue por outras três equipes globais.

Provedores de serviços de segurança gerenciados (MSSP)

Os MSSPs são contratados para gerenciar as operações de segurança de TI da organização, ou parte delas, permitindo que as equipes internas se concentrem nas tarefas diárias regulares. Os MSSPs oferecem a caça a ameaças como parte do serviço gerenciado, o que pode incluir serviços MDR, conforme detalhado acima.

Capacitadores da caça a ameaças

Detecção e resposta de endpoints/estendidas (EDR/XDR)

Para que os caçadores de ameaças identifiquem e investiguem possíveis atividades mal-intencionadas, eles precisam de informações e ferramentas de investigação. Trabalhe com EDR e XDR. Eles permitem que os caçadores vejam rapidamente as detecções suspeitas e as investiguem por completo.

Vale notar que o EDR oferece informações que são fornecidas pela solução de endpoint. Em contraste, o XDR consolida os sinais de toda a amplitude do ambiente de TI, incluindo soluções de segurança de firewall, dispositivos móveis, e-mail e nuvem. Dado que os adversários exploram toda e qualquer oportunidade de ataque, quanto mais longe você lançar a sua rede de sinais, mais cedo conseguirá detectá-los.

Um dos maiores desafios práticos das soluções EDR e XDR é o ruído: os caçadores de ameaças recebem tantos sinais que pode ser difícil ver a situação como um todo e separar alhos de bugalhos. Por isso é essencial combinar a sua solução EDR/XDR com uma poderosa proteção de endpoint que bloqueie mais ameaças de antemão, permitindo que sua linha de defesa se concentre em detecções menos frequentes e mais precisas.

A anatomia da detecção e resposta a ameaças

A caça a ameaças é um componente de uma operação muito mais ampla: a detecção e resposta a ameaças. Na Sophos, aplicamos uma estrutura de detecção e resposta a nossas caçadas que consiste em cinco componentes básicos:

1. Prevenção

Ter em vigor tecnologias de prevenção robustas e configuradas adequadamente (como uma solução de proteção de endpoint) evita que os invasores consigam se infiltrar na sua rede. Mais importante ainda é que isso também reduz o número de alertas de segurança que são gerados diariamente ou a cada hora. Com menos alertas para averiguar, a equipe de segurança pode se concentrar melhor nos sinais que realmente importam – nesse caso, adversários evasivos comandados por humanos.

2. Coleta de eventos de segurança, alertas e detecções

Os dados são o combustível que alimenta a caça e a análise de ameaças. Sem o tipo, o volume e a qualidade certa dos sinais, fica difícil para as equipes de operações de segurança identificar com precisão os indicadores de possíveis ataques – e dados sem contexto confundem os analistas na hora de tomar uma decisão convincente. Sem metadados significativos associados ao sinal, os analistas terão dificuldades para determinar se os sinais são malignos ou benignos.

3. Priorização dos sinais que importam

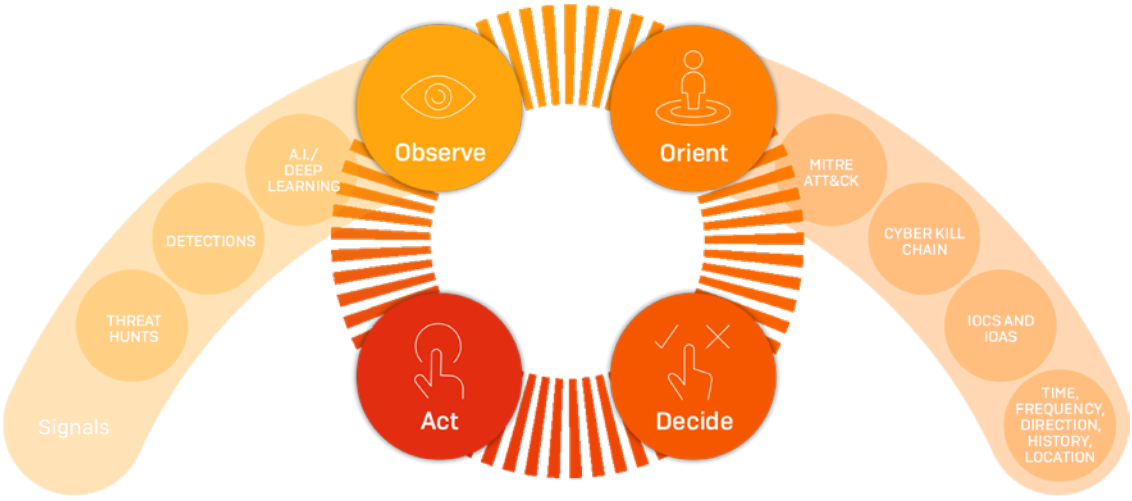
Para evitar ser soterrado por dados e perder a oportunidade de encontrar itens que exigem uma investigação mais minuciosa, você deve ser capaz de identificar os alertas que são importantes. Isso é mais difícil do que parece. O ideal é que você consiga melhorar ao máximo a relação entre sinal e ruído usando uma combinação de contexto que apenas os causadores do evento podem oferecer, juntamente com inteligência artificial automatizada. Porém, mesmo com a automação, não se trata de um processo simples.

4. Investigação

Assim que você isolar os sinais principais, será o momento de adicionar informações e medições que você descobriu nos modelos e estruturas da indústria para criar um patamar de confiança para comprovar seu comportamento maligno ou benigno.

Estrutura de investigação OODA

Analistas de segurança experientes frequentemente utilizam uma estrutura para conduzir suas investigações. Por exemplo, a equipe Sophos MDR usa uma metodologia investigativa conhecida como ciclo OODA. Isso permite que se engajem no ritmo, como mencionado, para garantir que todas as descobertas sejam testadas e comprovadas:



O ciclo OODA é uma estratégia militar que permite que nossas equipes sigam uma linha de raciocínio para entender por completo o evento e o comportamento gerado. As equipes podem desenvolver esse conhecimento e empregar a tomada de decisão e a intuição humanas para concluir se uma atividade mal-intencionada está presente no ambiente de um cliente, e, baseado nisso, decidir como agir.

Quando aplicam a estrutura OODA, os analistas de segurança da Sophos geralmente seguirão estes passos:

- **Observar** – o que você vê na detecção?
  - Observação das possíveis conexões externas e internas relacionadas à detecção.
  - Determinação de onde a detecção está ocorrendo e se os usuários finais estão associados a ela.
- **Orientar-se** – o que sabemos sobre a detecção?
  - Coleta de dados baseados em indícios.
  - Entendimento dos TTPs comuns ou específicos ao ataque ou agentes de ameaças. Um recurso utilizado para identificar TTPs é a estrutura MITRE ATT&CK, que será abordada em mais detalhes mais adiante no relatório.
  - Coleta de inteligência dos indicadores de ataques (IOA) e indicadores de comprometimento (IOC).
- **Decidir** – a detecção é maliciosa, suspeita ou benigna? É necessária uma ação?
- **Agir** – baseado nas etapas anteriores, o que você fará?
  - Mitigar – neutralizar – reprocessar – melhorar.

5. Ação

Isso é importante. Depois de determinar que está lidando com uma ameaça, você precisará fazer duas coisas que são igualmente importantes.

A primeira é mitigar o problema imediato e a segunda é lembrar-se de que você está provavelmente tratando apenas do sintoma do ataque e ainda precisa encontrar e neutralizar a causa primária. O primeiro ponto deve ser resolvido sem prejudicar sua capacidade de resolver o segundo ponto.

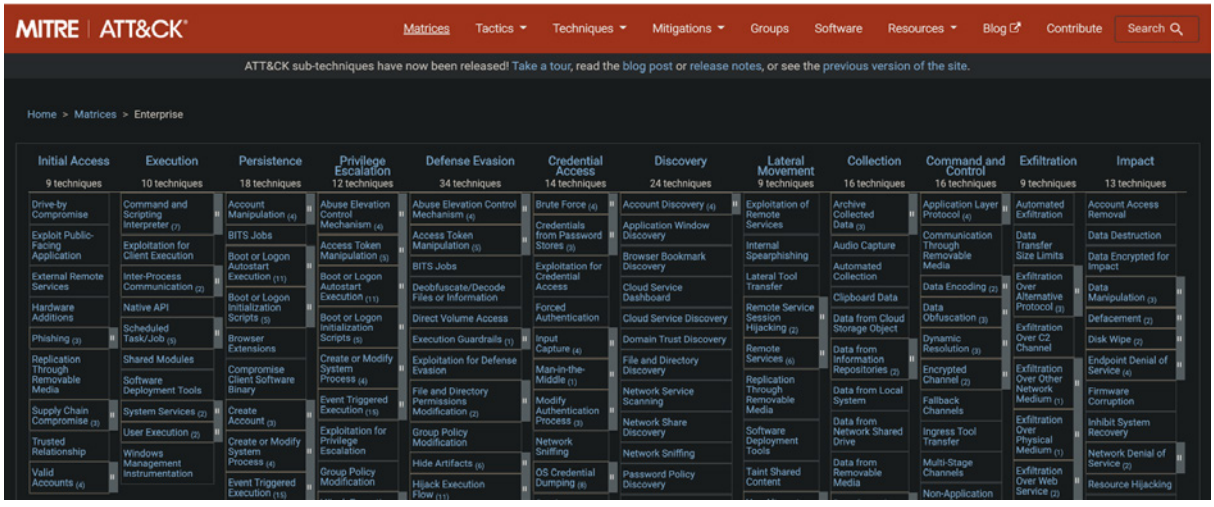
Às vezes, é suficiente colocar a máquina em quarentena ou desconectá-la da rede; já outras vezes, a equipe de segurança precisará ir mais fundo na rede para remover as ramificações do invasor.

Por exemplo, simplesmente porque você foi bem-sucedido em bloquear e remover o malware do seu sistema e não vê mais o alerta sobre ele, não significa que o invasor foi eliminado do seu ambiente.

Os caçadores de ameaças profissionais que analisam milhares de ataques sabem quando e onde procurar. Eles procuram por outras coisas que os invasores estejam fazendo, fizeram ou planejam fazer na rede – e neutralizam isso também.

Classificação de ameaças: a estrutura MITRE ATT&CK

Um recurso muito usado pelos caçadores de ameaças é a estrutura MITRE ATT&CK. Se você está na área de segurança cibernética, terá pelo menos ouvido falar nisso. Entre as muitas estruturas no mercado, a MITRE é uma base de conhecimentos de TTPs adversários acessível globalmente que se respalda em observações do mundo real e que é usada como alicerce para o desenvolvimento de metodologias e modelos específicos de ameaças. Ela permite que os caçadores de ameaças mapeiem os comportamentos dos invasores a uma infinidade de TTPs previamente identificados. Por sua vez, os caçadores podem estabelecer em que ponto no ciclo de vida se encontra o ataque, o que é crítico para o estágio "Orientar-se" na estrutura OODA.



Você pode obter informações mais detalhadas sobre a estrutura MITRE ATT&CK aqui.

Métodos de caça a ameaças

Esta seção analisará alguns métodos de caça a ameaças empregados comumente. Na Sophos, geralmente damos início a nossas buscas de duas formas diferentes.

Caça de ameaças com indícios

Na nossa organização, qualquer detecção que precise de mais investigação é revista por um analista de ameaças humano, que pode aplicar contexto comercial e raciocínio humano a qualquer situação. Eles observarão o comportamento, considerarão o contexto comercial previamente estabelecido, desenvolverão uma hipótese e trabalharão nela. Essa hipótese pode ser o engajamento ativo com o possível incidente ou a realização de um trabalho investigatório mais detalhado para consolidar seus conhecimentos sobre o problema em mãos.

Para fechar o ciclo, o analista vai aguardar e examinar os resultados da suposição e teste. Se uma investigação mais aprofundada for necessária, poderão repetir o ciclo até que cheguem a uma decisão. Se o evento tiver evoluído para um incidente ativo, o analista entrará no modo de resposta para combater a ameaça ativamente.

Caça de ameaças sem indícios

Enquanto a caça com indícios exige um ou mais sensores para detectar ou gerar um “sinal” de interesse, uma caça sem indícios é muito mais orgânica. Embora possamos usar nossos algoritmos de inteligência artificial para processar o grande número de dados que ingerimos, a caça a ameaças sem indícios é quase sempre conduzida por um analista de ameaças humano.

Ao invés de contar com um sinal inicial sistemático para nos alertar de que algo precisa ser investigado, nós realizamos consultas proativamente no patrimônio computacional do cliente, ou clientes. Isso pode acontecer por inúmeros motivos, entre eles:

- Um cliente na mesma indústria vertical foi feito alvo de um jeito particular, e queremos realizar uma diligência prévia para garantir que os mesmos agentes de ameaças não fiquem tentados a atacar nossos outros clientes
- O SophosLabs informou a equipe de MDR sobre um ataque significativo tendo clientes como alvo, no mesmo mercado vertical ou com propriedades semelhantes
- Um evento significativo ocorreu no cenário da segurança, e queremos averiguar se algum de nossos clientes foi afetado

Estudo de caso: A caça ao ransomware que desvendou um histórico cavalo de Troia bancário

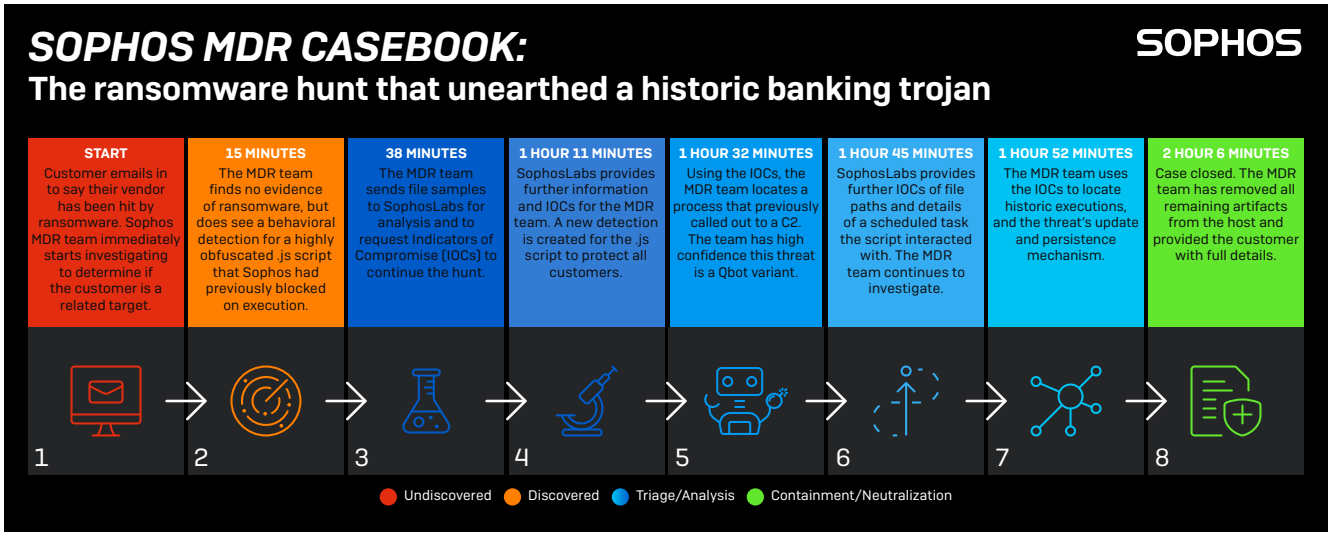
Agora que descrevemos as peculiaridades da caça a ameaças, vamos acompanhar a caça a uma ameaça em ação. Como investigado pela equipe Sophos MDR, esse caso é um ótimo exemplo de como a caça a ameaças pode revelar resultados inesperados. Nesse caso, um cliente entrou em contato dizendo que um fornecedor com quem trabalhava havia sido vítima de um ransomware, e o cliente estava preocupado que ele talvez também pudesse ter sido infectado.

A equipe Sophos MDR começou suas investigações imediatamente, trabalhando com nossos peritos do SophosLabs, que rapidamente perceberam que não havia indícios de ransomware. Nesse ponto, muitas equipes talvez fechassem o caso e o dessem por encerrado. Contudo, a equipe Sophos MDR continuou investigando e descobriu um cavalo de Troia histórico.

O cliente pode descansar sabendo que não havia sido afetado pelo ransomware e que um cavalo de Troia histórico havia sido totalmente removido – um resultado que não se concretizaria sem intervenção especializada.

Como mostra a história, ainda que ransomwares sejam a ameaça que mais ocupa nossa mente, é crucial que também estejamos alertas aos ataques que preferem se esconder nas sombras.

Em duas horas e seis minutos, o incidente completo havia sido investigado e eliminado.



Para se aprofundar mais nesse caso, leia o artigo aqui.

Preparando-se para a caça a ameaças: cinco etapas que levam a bons resultados

Você agora certamente já deve ter adquirido uma boa noção dos fatores relacionados à caça a ameaças. Contudo, antes de começar, é essencial assegurar que a sua organização esteja bem equipada para seguir com eficiência.

1. Entenda a maturidade das suas operações de segurança cibernética atuais

Antes de poder entender seus possíveis adversários, você precisa entender o estado das operações atuais de segurança cibernética. Mapear seus processos a um modelo de maturidade de segurança cibernética (como o CMMC) é uma ótima maneira de estabelecer se você está bem equipado, ou não, para começar a caça a ameaças. Uma boa ideia também é fazer uma auditoria da sua postura de segurança para determinar qual sua suscetibilidade a ameaças.

2. Decida como deseja sair no encalço das ameaças

Assim que estabelecer a maturidade de sua segurança, poderá decidir se deseja manter a caça a ameaças com seu pessoal interno, terceirizá-la totalmente ou combinar as duas opções.

3. Identifique lacunas na tecnologia

Examine suas ferramentas existentes e identifique o que mais precisa fazer para capturar com eficiência. Qual a eficácia da sua tecnologia de prevenção? Ela tem ou aceita recursos para caça e captura de ameaças proporcionados por EDR/XDR?

4. Identifique lacunas em habilidades

A caça a ameaças é complexa e exige habilidades especializadas. Se você não tem esse tipo de experiência entre seu pessoal interno, explore a possibilidade de promover cursos de treinamento para ajudar a desenvolver a especialização necessária. Considere também a possibilidade de trabalhar com um provedor terceirizado para complementar suas equipes.

5. Desenvolva e implemente um plano de resposta a incidentes

Antes de começar a caça a ameaças, é essencial que você tenha um plano de resposta completo em vigor para garantir que as respostas a incidentes sejam medidas e controladas. Ter um plano de resposta bem-preparado, bem-estudado e bem-entendido a que todos os envolvidos tenham acesso e possam colocar em ação imediatamente reduzirá drasticamente o impacto de um ataque na sua organização.

Um bom plano de resposta a incidentes deve descrever protocolos de preparação, detecção e relatório, triagem e análise, contenção e neutralização, e atividades pós-incidente. Para ver dicas sobre como criar um plano de resposta a incidentes eficiente, consulte o nosso guia de resposta a incidentes.

Para obter diretrizes práticas sobre como se preparar para realizar uma caça a ameaças, visite a Sophos Threat Hunting Academy.

Como a Sophos pode ajudar

Como já mencionamos, a caça a ameaças eficiente é incrivelmente complexa e requer tecnologias next-gen e perícia humana altamente especializada. Felizmente, a Sophos oferece suporte aos seus objetivos independentemente do nível de maturidade da sua segurança cibernética.

Prevenindo que ameaças violem sua rede – Sophos Intercept X Endpoint

Os caçadores de ameaças só podem cumprir seu papel com eficiência se não forem bombardeados com alertas de segurança. Uma maneira de atingir isso é introduzindo tecnologias de prevenção de ponta para que as equipes de defesa se concentrem em detecções menos frequentes e mais precisas, e agilizem os processos posteriores de investigação e resposta. Trabalhe com o Sophos Intercept X Endpoint.

O Sophos Intercept X é a solução de segurança de endpoint líder no setor que reduz a superfície de ataque e previne sua incidência. Combinando anti-exploit, anti-ransomware, IA com Deep Learning e tecnologia de controle, ele bloqueia as ameaças antes que afetem os seus sistemas. O Intercept X usa uma abordagem abrangente de defesa para proteger endpoints, em vez de contar com uma técnica básica de segurança.

Os recursos de prevenção para proteção de endpoints do Sophos Intercept X bloqueia 99,98% das ameaças (pontuação média da AV-TEST, jan-nov 2021). Seu pessoal de defesa pode se concentrar nos sinais suspeitos que exigem a intervenção humana.

Você pode obter mais informações sobre o Intercept X Endpoint ou fazer uma avaliação aqui.

Conduzindo sua própria caça a ameaças – Sophos XDR

Desenvolvido para analistas de segurança que trabalham em equipes SOC dedicadas e administradores de TI que focam em segurança e outras responsabilidades de TI, o Sophos XDR capacita seu pessoal para detectar, investigar e responder a incidentes em seus endpoints, servidores, firewalls, cargas de trabalho na nuvem, e-mails, dispositivos móveis e mais.

Acesse imediatamente as informações que realmente importam utilizando uma biblioteca de modelos personalizados e prontos para uso que abrangem diferentes cenários de caça a ameaças e operações de TI – ou crie o seu próprio modelo. Com acesso a dados do dispositivo em tempo real, até 90 dias de dados em disco, 30 dias de dados armazenados no repositório do Sophos Data Lake na nuvem e uma lista gerada automaticamente de itens suspeitos, você sabe exatamente de onde começar.

Se quiser experimentar o Sophos XDR para conduzir a sua própria caça a ameaças, a Sophos lhe dá as ferramentas de que você precisa para sair no encalço de ameaças avançadas e manter a higiene de suas operações de segurança. Você pode iniciar uma avaliação interna de produto (se tiver uma conta do Sophos Central) ou fazer a avaliação do Sophos Intercept X, o qual inclui o XDR.

Desempenhando a caça a ameaças como um serviço totalmente gerenciado ou complementar para a equipe – Sophos MDR

O Sophos MDR é uma solução MDR premiada de grande abrangência e versatilidade que oferece a expertise e proficiência das equipes Sophos de analistas de segurança e sua vasta habilidade em lidar com ambientes de rede e nuvem. A Sophos se torna irrefutavelmente uma extensão das suas operações de segurança, adicionando seu amplo portfólio à sua experiência.

A equipe de caçadores de ameaças e peritos em respostas do Sophos MDR irá:

- Capturar ameaças de forma proativa, validando ameaças e incidentes potenciais
- Usar todas as informações disponíveis para determinar o escopo e a gravidade das ameaças
- Aplicar o contexto comercial apropriado às ameaças validadas
- Iniciar ações para deter, conter e neutralizar as ameaças remotamente
- Oferecer conselhos práticos para tratar da causa primária dos incidentes recorrentes

Mesmo que a sua organização tenha um centro de operações de segurança mais experiente, você certamente vai buscar outro par de olhos para monitorar seus ambientes e garantir que nada passe despercebido. O Sophos MDR uni a caça a ameaças com a proteção de endpoint e ainda oferece supervisão e expertise no dia a dia. Seus ativos na rede e na nuvem são prioridade máxima para os analistas de rede da Sophos e caçadores de ameaças que monitoram e ativamente reparam e neutralizam ameaças por você.

Com um bom serviço MDR, você e a sua organização podem ficar tranquilos, sabendo que uma equipe de profissionais altamente treinados estará monitorando constantemente a sua organização, sempre no encalço de ameaças, investigando atividades suspeitas e respondendo a possíveis incidentes. Neste cenário incessantemente crescente de ameaças virtuais, a sensação de tranquilidade se instaura quando você sabe que está trabalhando com uma equipe totalmente voltada à segurança cibernética.

Para conversarmos sobre como o Sophos MDR pode dar suporte à sua organização, fale com um representante da Sophos ou solicite uma ligação. Enquanto isso, acompanhe os recentes casebooks e pesquisas em MDR.

Vendas na América Latina
E-mail: latamsales@sophos.com

Vendas no Brasil
E-mail: brasil@sophos.com

22-08-08 WP-PTBR (PC)

SOPHOS