DARKTRACE

Resposta Cyber AI: Relatório de Ameaças 2019

Introdução

Cada vez mais, as empresas enfrentam fatores de risco extremamente urgentes nesta era de ameaças cibernéticas automatizadas e dinâmicas. Esses riscos têm aumentado drasticamente nos últimos anos, à medida que as ameaças se desenvolvem e se tornam mais avançadas e com os negócios digitais crescendo continuamente em complexidade, diversidade e escala.

No passado, quando as ameaças eram menos sofisticadas e as redes eram mais previsíveis, uma abordagem tradicional de segurança era adequada para fazer frente as ameaças cibernéticas. Ao configurar ferramentas de segurança utilizando uma combinação de regras ou assinaturas, as equipes de segurança procuram detectar ameaças definindo-as antecipadamente como "benignas" ou "malignas", contando com reproduções de ataques que foram concebidos sob a forma de uma regra, ou que foram observados "em ação" e aos quais se aplicou engenharia reversa para futura detecção.

No entanto, a frequência cada vez maior de novos ataques externos e ameaças internas, juntamente com a complexidade e sutileza dos comportamentos diários em uma empresa, desarmou gradualmente as equipes de segurança que ainda dependem dos controles tradicionais. As defesas tradicionais não detectam as novas táticas e técnicas de cibercriminosos sofisticados, que agora podem se camuflar no ruído da rede e varrer infraestruturas grandes e complexas em segundos.

Como a entrada de novas ameaças é inevitável, a atenção do setor se voltou à questão de como os defensores cibernéticos podem se preparar para detectar e responder a ameaças emergentes que já estão dentro da empresa, mas que podem ser resolvidas antes de se tornarem uma crise. Para acompanhar o ritmo, líderes empresariais e equipes de segurança tem recorrido à inteligência artificial.

A aplicação única da inteligência artificial da Darktrace, por sua vez, aprende o "padrão de vida" ('pattern of life') normal de empresas individuais e identifica desvios sutis indicativos de uma ameaça, seja ela conhecida ou desconhecida, externa ou interna, sutil ou dinâmica. Através do aprendizado contínuo e da adaptação em tempo real à novas evidências, a inteligência artificial da Darktrace aponta indicadores de ameaças com antecedência, sem depender de regras, assinaturas ou suposições iniciais, que de outra forma passariam despercebidos.

Resumo

Este relatório detalha sete estudos de caso de ataques que foram interceptados e neutralizados pela inteligência artificial de defesa cibernética, incluindo ataques de ameaças internas, ransomware e IoT.

Embora todos os cenários de ameaças fossem diferentes, alguns dinâmicos e outros lentos e furtivos, em todos os casos os indicadores sutis de atividades suspeitas eram detectáveis apenas com a inteligência artificial da Darktrace, que aprende o que é normal para o ambiente de negócios e responde de maneira autônoma a ataques antes que ocorram danos.

Contra-ataque com a Darktrace Antigena

À medida que a lacuna de habilidades é ampliada, e o volume e a velocidade dos ataques aumentam, a IA não é apenas essencial na detecção de ameaças emergentes, mas também é usada para potencializar a resposta da linha de frente de uma organização. A Darktrace Antigena é a IA que pode contra-atacar em tempo real, dando tempo para a equipe de segurança reagir.

Com sua compreensão avançada e evolutiva do "padrão de vida" normal de cada usuário, dispositivo e grupos de dispositivos associados a uma empresa, a IA da Darktrace pode não apenas responder aos primeiros indicadores de uma ameaça cibernética antes que eles causem danos, mas também é capaz de fazer isto de maneira altamente direcionada. Em vez de gerar quarentenas que serviriam apenas para causar mais interrupções, a Darktrace Antigena (solução de resposta cibernética autônoma do sistema) funciona impondo cirurgicamente o "padrão de vida" normal a um dispositivo infectado ou funcionário descontente, neutralizando a ameaça em segundos e mantendo as operações normais.

Na luta contra os criminosos cibernéticos avançados, a IA da Darktrace devolve o controle aos defensores, transformando até mesmo a organização mais complexa e vulnerável em uma organização resiliente e autodefensiva.

Ameaça interna

Um funcionário escaneando a rede em busca de vulnerabilidades

Malicioso e persistente

As ameaças internas são um dos vetores de ataque mais perigosos e comuns nas empresas, sejam ou não maliciosas. Membros internos mal-intencionados representam uma ameaça especialmente significativa para os negócios, pois seu acesso privilegiado e conhecimento da rede permitem que eles realizem missões de ataque prolongadas e retirem ou manipulem silenciosamente dados críticos sem levantar suspeitas.

A IA da Darktrace identificou e neutralizou um membro interno mal-intencionado em uma grande empresa de investimento na África do Sul. A IA de autoaprendizagem conteve uma ameaça persistente enquanto essa passava por vários estágios da cadeia de ataque, desde o reconhecimento até a gravação e execução de script. Com a aprendizagem continua, a Antigena adaptou-se a ameaça à medida que ela avançava e a conteve com eficácia em cada etapa.

Comportamento suspeito

A etapa de reconhecimento começou com um laptop executando "ping" em centenas de endereços IPs internos para identificar quais estavam ativos. Em seguida, varreu a rede em busca de nomes de máquinas responsivas e escaneou elas em busca de canais abertos de comunicação. A IA da Darktrace sinalizou o comportamento suspeito como atividade incomum de varredura de rede e solicitou a Antigena a tomar uma ação. Com base em sua avaliação dinâmica de ameaças, a Antigena decidiu impor o "padrão de vida" do grupo do dispositivo por uma hora, evitando que o laptop desviasse de seu comportamento anterior ou do comportamento de seus pares.

No entanto, algumas horas depois, a ameaça retornou. O laptop começou a executar comandos em centenas de outros computadores internos no intervalo de IPs identificado inicialmente. Isso envolvia mover arquivos de script multifuncionais e usar uma ferramenta de administração remota. Esses programas podem ser explorados para localizar informações e documentos confidenciais ou para abrir um backdoor para um invasor externo executar um sequestro.

> A Darktrace Antigena decidiu impor o "padrão de vida" do grupo do dispositivo por uma hora

Antigena entra em ação

Nenhuma outra gravação de arquivos semelhante foi observada em toda a rede durante esse período, o que se mostrou ser altamente incomum para a IA da Darktrace. Com a sua compreensão das ameaças no contexto da rede e da sua resposta autônoma anterior, a Antigena decidiu bloquear todas as conexões de saída usando o canal de transferência de arquivos SMB, contendo instantaneamente qualquer movimentação lateral pela rede.

Após a neutralização da ameaça, a equipe de segurança pôde investigar e confirmar que o laptop pertencia a um membro da equipe de TI que estava usando uma ferramenta de varredura não legítima para buscar pontos vulneráveis na rede. Esse é um exemplo especialmente revelador do poder da IA da Darktrace e de como a Antigena pode intervir em diferentes etapas de uma cadeia de ataques e neutralizar ameaças no estágio inicial.

Cavalo de Troia de dia zero

Downloads e conexões suspeitas

Nova variedade de malware

Embora ferramentas de segurança legadas possam frequentemente identificar ameaças conhecidas que já foram descobertas, a IA pode identificar de maneira única os sinais sutis e tênues de uma ameaça cibernética ainda não conhecida. Essa capacidade tornou-se necessária nos últimos anos, à medida que criminosos cibernéticos avançados continuam a desenvolver novas táticas, técnicas e procedimentos desenvolvidos especificamente para fugir dos controles pré-programados com assinaturas de ataques anteriores.

A capacidade da Darktrace de reagir a esses indicadores sutis foi fundamental para um fabricante americano de controles industriais de IoT quando foi atingido por um cavalo de Troia de dia zero.

Às 13h30 de uma quinta-feira, a IA alertou ao gerente de TI da empresa sobre um download suspeito de um arquivo chamado "OfficeActive.bin". Embora o arquivo se parecesse com um produto da Microsoft, a Darktrace indicou que o arquivo estava sendo baixado de uma fonte não identificada que era 100% incomum na rede.

> Embora o arquivo parecesse com um produto da Microsoft, a Darktrace indicou que o arquivo estava sendo baixado de uma fonte não identificada

Desenvolvimento de confiança na resposta autônoma da IA

Na época, a Antigena foi configurada no "Modo Passivo", um modo inicial que restringe a IA a comunicar o que teria feito em resposta à ameaça, sem realmente agir, permitindo que a equipe desenvolvesse confiança na tomada de decisões do sistema. A equipe de TI pôde observar como a Antigena teria interrompido o ataque em um estágio inicial e também como ela se adaptou a uma nova ameaça à medida que essa se intensificava.

Em resposta ao padrão altamente incomum da atividade, a Antigena recomendou primeiro a imposição do "padrão de vida" do grupo do dispositivo por duas horas, o que interromperia a ameaça enquanto as operações normais eram mantidas.

Ao observar mais downloads suspeitos, a Antigena aumentou sua resposta, impondo o "padrão de vida" individual do dispositivo por cinco minutos. Quando o dispositivo tentou fazer uma nova conexão externa, a Antigena respondeu novamente, sugerindo que a IA bloqueasse cirurgicamente todas as conexões de saída do dispositivo por uma hora.

Remediação da ameaça

Poucos minutos após a identificação da alerta, o gerente de TI havia contatado o usuário e realizado uma recomposição de emergência para corrigir a ameaça na máquina. Todo o processo foi concluído em 20 minutos. Após a neutralização da ameaça, o gerente de TI copiou a URL e o nome do arquivo do cavalo de Troia no analisador Virus Total para verificar se a ameaça havia sido observada e registrada em outro local. A busca não retornou resultados, confirmando que realmente se tratava de um cavalo de Troia de dia zero, descoberto exclusivamente pela IA da Darktrace.

Invasão IoT: CCTV

Espionagem corporativa?

Câmera de segurança comprometida

A crescente conectividade dos dispositivos usados no dia-a-dia introduziu ainda mais vulnerabilidades nas empresas. Os dispositivos de IoT, geralmente projetados com controles básicos de segurança não integrados, são rotineiramente visados por agentes de ameaças e usados como portas de entrada para a rede.

Em uma consultoria de investimentos japonesa, a Darktrace descobriu que um sistema de CCTV conectado à Internet havia sido infiltrado por invasores desconhecidos. Dessa forma, os criminosos obtiveram um ponto de entrada para a rede e puderam assistir a todas as gravações de vídeo da câmera. Instalada para monitorar todo o espaço de trabalho, desde o escritório do CEO até a sala de reuniões, a câmera se tornou um risco à segurança.

> A IA contra-atacou rapidamente, impedindo uma violação séria

Reação rápida

A IA da Darktrace detectou rapidamente que algo estava errado. Observou-se grandes volumes de dados movendo-se no servidor de CCTV não criptografado, pois o invasor coletava dados para preparar a extração de informações confidenciais.

No momento em que o invasor tentou extrair os dados, a Antigena tomou medidas defensivas rápidas e precisas. O sistema decidiu bloquear cirurgicamente a movimentação de dados do dispositivo para um servidor externo, enquanto ainda permitia que a CCTV operasse na capacidade desejada.

A IA contra-atacou rapidamente, impedindo uma violação séria de informações confidenciais no mercado. Ao tomar medidas adequadas para conter o ataque em um estágio inicial, a Antigena deu tempo à equipe de segurança para investigar e corrigir a ameaça antes que qualquer dano fosse provocado.

Invasão IoT: armário inteligente

Dados confidenciais do cliente como alvo

Vulnerabilidade de IoT

Em um parque de diversões na América do Norte, um "agente de ameaças" tentou roubar dados confidenciais de clientes por meio de um dispositivo IoT vulnerável: um armário "inteligente" usado pelos visitantes para guardar pertences pessoais.

Como parte de sua configuração padrão, o armário inteligente estabelecia regularmente contato com a plataforma online de terceiros do fornecedor. O "agente de ameaças" identificou a origem desse processo automatizado e sequestrou-o para comprometer o dispositivo.

Silencioso e lento

A IA da Darktrace detectou o ataque logo após o armário começar a enviar uma quantidade incomum de dados não criptografados para um site externo atípico. As conexões foram programadas de acordo com as comunicações regulares do dispositivo com a plataforma do fornecedor, sugerindo que esse foi um ataque "silencioso e lento" projetado especificamente para se esquivar das defesas de segurança baseadas em regras.

Ao analisar continuamente as comunicações em relação ao comportamento anterior do armário e de seus pares, a IA da Darktrace determinou que uma resposta cibernética era necessária. Em poucos segundos, a Darktrace Antigena agiu de maneira inteligente, bloqueando todas as conexões de saída do dispositivo comprometido, dando tempo à equipe de segurança para corrigir a ameaça e evitar a extração.

Nesse parque de diversões e em outros, a IA cibernética da Darktrace neutralizou incontáveis ataques "silenciosos e lentos" em estágio inicial. Com a aprendizagem em tempo real o sistema detecta ameaças sutis que outras ferramentas não percebem. Ele verifica continuamente sua compreensão à luz de novas evidências e gera ações autônomas que se adaptam à ameaça à medida que ela avança.

Ransomware

Rápido e grave

Extorsão automatizada

Às 19h05 de sexta-feira, um funcionário de uma grande empresa de telecomunicações acessou seu e-mail pessoal usando um smartphone corporativo e foi levado a baixar um arquivo malicioso contendo ransomware. Segundos depois, o dispositivo começou a se conectar a um servidor externo na rede Tor.

A IA da Darktrace respondeu em instantes. Apenas nove segundos após o início das atividades de criptografia SMB, a Darktrace emitiu um alerta prioritário informando que a anomalia exigia investigação imediata. Como o comportamento persistiu nos próximos segundos, a Darktrace revisou sua decisão e ativou a Antigena.

Como a equipe de segurança havia saído do escritório para o final de semana, a Darktrace Antigena respondeu de maneira autônoma, interrompendo todas as tentativas de gravação de arquivos criptografados em compartilhamentos de rede. Isso neutralizou instantaneamente a ameaça antes que ela pudesse se espalhar pela ampla infraestrutura da empresa de telecomunicações, dando tempo para a equipe de segurança agir.

À medida que variedades automatizadas de ransomware continuam a surgir na Dark Web e em redes corporativas em todo o mundo, as organizações precisam contra-atacar para acompanhar o ritmo. Assim como em outras situações, a resposta cibernética da IA da Darktrace se tornou um componente essencial nessa batalha, contendo ataques de ação rápida antes que eles tivessem tempo de criptografar dados críticos e interromper os negócios.

Spear Phishing

Um ataque direcionado por e-mail

Ataque por e-mail

Um município dos EUA foi vítima de um ataque direcionado por e-mail. Embora muitos ataques de phishing sejam campanhas direcionadas, essa apresentava as marcas de um cibercrime coordenado e sofisticado. Os e-mails foram bem elaborados e personalizados para o destinatário pretendido. O "agente da ameaça" também havia tido acesso à lista de endereços da cidade, pois o ataque foi entregue aos destinatários em ordem alfabética, de A a Z.

Ainda assim, embora cada e-mail parecesse inofensivo e fosse personalizado para o destinatário, todas as mensagens continham uma carga maliciosa oculta por trás de um botão disfarçado como um link para Netflix, Amazon e outros serviços confiáveis.

> A Antigena identificou a campanha na letra "A", enquanto as ferramentas legadas despertaram para a ameaça na letra "R"

Links ocultos

A IA da Darktrace conseguiu analisar esses links ocultos em conexão com os "padrões de vida" normais dos destinatários pretendidos na rede. Quando o primeiro e-mail foi enviado, a Antigena reconheceu imediatamente que nem o destinatário, nem ninguém em seu grupo de amigos ou no restante da equipe da cidade, havia acessado esse domínio anteriormente. A Darktrace Antigena instantaneamente gerou uma alerta de alta confiança e sugeriu que cada link fosse bloqueado autonomamente quando entrasse na rede.

Curiosamente, o fato da Antigena ter sido implementado no "modo passivo" forneceu evidências claras e concretas da capacidade do sistema de impedir ataques sutis que outras ferramentas não perceberiam. Enquanto a Antigena detectava e procurava neutralizar a campanha na letra "A", as ferramentas legadas da equipe de segurança detectaram a ameaça na letra "R". Em "modo ativo", a Antigena teria neutralizado o ataque antes que ele atingisse um o primeiro usuário.

Ataque à cadeia de fornecimento

Um impostor explorou relacionamentos de confiança

Conta de e-mail invadida

Alguns dos cibercriminosos mais talentosos aprenderam que a maneira mais fácil de entrar na empresa geralmente é passar pela porta da frente, desde que eles possam obter a confiança de um usuário legítimo. Ao sequestrar os detalhes da conta de um colega, parceiro de negócios ou fornecedor confiável ao longo da cadeia de fornecimento, os agentes de ameaças podem levar os destinatários a clicarem em um link malicioso ou a transferirem milhões para fora da empresa.

A IA da Darktrace identificou um desses ataques que teve como alvo um estúdio de produção cinematográfica em Los Angeles, depois que os detalhes da conta de um fornecedor de confiança foram comprometidos.

Os detalhes da conta podem ser usados para muitos propósitos criminosos mas, nesse caso, parece ter sido usado para ler o histórico de correspondência do contato com um funcionário do estúdio. Depois de analisar os tópicos anteriores e aprender como o contato e o funcionário se comunicavam normalmente, ele enviou uma resposta plausível ao último e-mail do funcionário.

> O e-mail era convincente e refletiu o estilo e o tom da escrita do contato

Acreditar nisso ou não?

O e-mail era convincente e refletiu o estilo e o tom da escrita do contato, além de fazer sentido no contexto do relacionamento e das discussões anteriores. A mensagem incluía também um link malicioso que pareceria inofensivo para qualquer funcionário sensato que recebesse um link de um contato familiar em uma empresa conhecida. Esses tipos de ataques são cada vez mais comuns e muito difíceis de detectar.

A IA da Darktrace detectou os indicadores fracos que revelaram que esse "contato de confiança" era uma conta invadida e controlada por um invasor. A resposta da IA imunizou a rede com o conhecimento de que o e-mail e seu conteúdo estavam fora do "padrão de vida" do suposto remetente. O funcionário foi alertado e a carga maliciosa foi neutralizada.

Essencialmente, a decisão da Antigena foi bascada no fato de que esse link específico seria incomum tanto para o remetente quanto para o destinatário, considerando-se suas comunicações anteriores e os "padrões de vida" normais do funcionário na rede. A equipe de segurança se sentiu confiante em sua postura de segurança, sabendo que a IA da Darktrace não tratava o destinatário na rede como um mero endereço de e-mail. Em vez disso, a Antigena reconhece que o escopo completo do "padrão de vida" de um funcionário é muitas vezes manifestado em cantos dispares da rede e de uma maneira que pode ser correlacionada e analisada de modo favorável pela IA cibernética.

Sobre a Darktrace

A Darktrace é a empresa líder mundial em IA para defesa cibernética. Com milhares de clientes em todo o mundo, o Enterprise Immune System detecta e combate ataques cibernéticos em tempo real. A tecnologia de IA aprende de forma autônoma e protege ambientes Cloud, SaaS, redes corporativas, IoT e sistemas industriais contra ameaças e vulnerabilidades cibernéticas, desde ameaças internas e ransomware até ataques furtivos e silenciosos. A Darktrace tem mais de 800 funcionários e 40 escritórios em todo o mundo. A empresa está sediada em São Francisco e Cambridge, no Reino Unido.

Contato

Brasil: +55 11 972 422 011
Estados Unidos: +1 (415) 229 9100
Europa: +44 (0) 1223 394 100
Ásia-Pacífico: +65 6804 5010
info@darktrace.com | darktrace.com
@darktrace