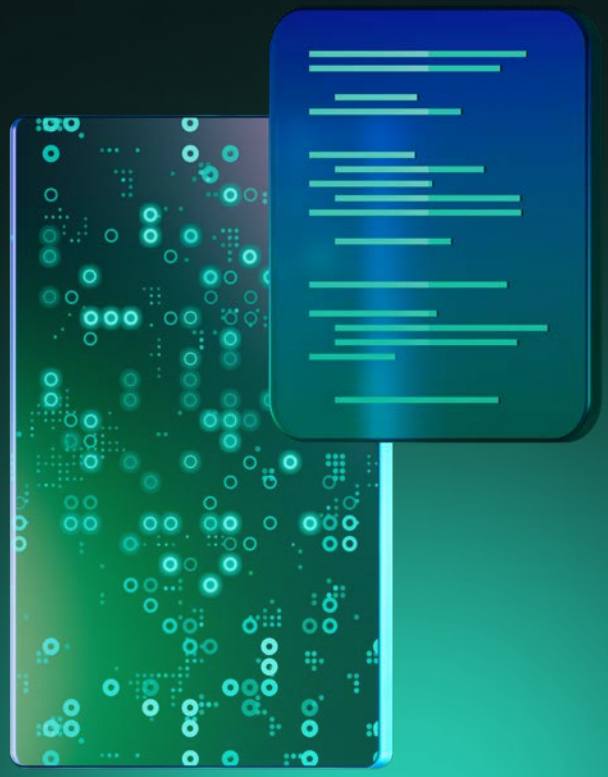
kaspersky

Como a Kaspersky AI ajuda na proteção de endpoints



Como a Kaspersky AI ajuda na proteção de endpoints

O cenário atual de ameaças está mais perigoso do que nunca. Os crimes cibernéticos são um setor especializado há muito tempo e os criminosos estão constantemente fabricando novos malwares e desenvolvendo novas técnicas de ataque. A coleção da Kaspersky conta agora com mais de 2,1 bilhões de amostras de vírus maliciosos, uma cifra que quase duplicou nos últimos cinco anos. Os sistemas automatizados detectam mais de 467 mil novas ameaças diariamente, e esse número também duplicou nos últimos anos.

A situação na qual as ameaças de malware podem ser combatidas com tecnologias tradicionais já não corresponde à realidade. Por isso, a Kaspersky já usa a IA há 20 anos e tem aprimorado continuamente suas tecnologias desde então. A empresa acredita em uma abordagem multicamadas para a cibersegurança, na qual cada camada pode ser reforçada com o uso da IA.

Com relação à proteção de endpoints, a primeira camada é a análise estatística, que corresponde à primeira linha de defesa. As soluções de endpoints da Kaspersky monitoram possíveis fontes de contaminação, como surfar na internet, e-mails, redes locais, pen drives e unidades USB removíveis e novos aplicativos, dependendo da plataforma e do sistema operacional. Todos os objetos recebidos são verificados pelos mecanismos, equipados com diversas tecnologias de IA.

Os mecanismos da Kaspersky extraem metadados e dissecam o objeto para coletar características, parâmetros exclusivos que descrevem esse objeto. Essas características (milhares delas, na verdade) são processadas pelos modelos de aprendizagem de máquina (ML) com base nos conjuntos de árvore de decisão. Esses modelos preditivos são treinados em conjuntos de dados com milhões de exemplos de treinamento selecionados cuidadosamente, usando algoritmos como floresta aleatória ou boost gradiente, e compostos por um conjunto de decisões. Um desses modelos, PE Forest, detecta dezenas de milhares de arquivos maliciosos diariamente. Esses modelos são usados na nuvem e também no ambiente de borda.

Outra tecnologia vital usada para análise estatística é hashing de semelhança. Também chamado de hashing sensível à localidade (LSH), esse é um método de IA usado para detectar arquivos maliciosos com grau de similaridade. Para criar hashes de similaridade, o sistema extrai características do arquivo e usa aprendizado de projeção ortogonal para escolher as características mais importantes. Em seguida, a compactação baseada em aprendizagem de máquina (ML) é aplicada de modo que os vetores de valor de características semelhantes sejam transformados em padrões semelhantes ou idênticos. Esse método fornece uma generalização robusta e reduz consideravelmente o tamanho da base de registros de detecção, pois um registro pode detectar uma família inteira de malware polimórfico (ou seja, malware que altera seu corpo a cada vez que se replica, enquanto mantém a funcionalidade do núcleo).

A infraestrutura distribuída complexa disponível no Kaspersky Security Network (KSN), combinada com sistemas de processamento automático agem como um super cérebro cibernético, coletando e analisando dados de ameaças de milhões de usuários voluntários participantes para identificar ameaças instantaneamente. A tecnologia analisa milhões de amostras diariamente e processa bilhões de notificações do KSN, agregando inteligência sobre ameaças relativa a objetos suspeitos usando diversas tecnologias de IA. O Sistema de Reputação Astaea agrega todas as estatísticas com meta-informação sobre objetos suspeitos em todo o mundo em tempo real. A reputação dos objetos é então calculada de acordo com a análise, e informações sobre novas ameaças de malware são imediatamente disponibilizadas para todos os usuários no KSN. Se o sistema Astrea não tiver informações suficientes sobre um objeto para tomar uma decisão, irá repetir a análise tão logo informação adicional seja coletada.

Do mesmo modo, o Sistema de Detecção de Hash atua como outra tecnologia baseada em ML para detectar variações de malware. O componente de nuvem do sistema agrega várias características de arquivos de diferentes origens, incluindo sistemas automáticos de processamento de malware em laboratório. Um algoritmo de ML é então usado para localizar características comuns em um grupo inteiro de arquivos maliciosos semelhantes. Com base nessas características, os Hashes por Similaridade (SH) são calculados e disponibilizados para us usuários do KSN. De acordo com a telemetria da Kaspersky, essa tecnologia protege centenas de milhares de clientes contra novos malwares diariamente.

Além disso, o ML na nuvem para Android é uma tencologia baseada na nuvem que protege usuários de smartphones Android. O modelo é treinado com milhões de amostras de malware de dispositivos móveis e pode detectar aplicativos malware maliciosos com alta precisão, abrangendo mais de 90% de ameaças novas e desconhecidas e impedindo milhões de ataques contra clientes Kaspersky anualmente.

Os sistemas de processamento automático interno da Kaspersky também usa IA abrangentemente. Além das tecnologias mencionadas, o sistema usa modelos ML de alta capacidade que não podem ser executados em endpoints ou na nuvem (devido aos altíssimos requisitos de recursos), mas são extremamente poderosos e precisos. Por exemplo, as soluções usam modelos ML baseados em redes neurais treinadas com centenas de milhões de amostras legítimas e maliciosas para localizar novo malwares e também prevenir falsos positivos. O modelo detecta mais de 80% dos novos arquivos maliciosos através de sistemas de processamento automático. Outros modelos ML analisam logs comportamentais e tráfego de seus sandboxes. A detecção de objetos maliciosos é fornecida rapidamente para endpoints protegidos pelas suas soluções, usando serviços KSN baseados em nuvem.

O modelo de detecção de phishing da web patenteado da Kaspersky é treinado com um extenso conjunto de dados com milhões de amostras para detectar páginas da web maliciosas, com base no conteúdo e metadados. A solução funciona com base na extração de insights avançados sobre padrões que definem páginas de phishing, garantindo uma identificação robusta de ameaças e permitindo a detecção de centenas de milhares de recursos de phishing da web anualmente. Teste e mecanismos de filtragem especializados abrangentes são projetados para minimizar falsos positivos, além de manter a já conhecida precisão líder da indústria.

A Kaspersky também usa IA para detectar domínios maliciosos e de phishing baseados nas relações da infraestrutura com domínios conhecidos desses tipos. A solução constrói um gráfico de domínios baseado nos metadados e resoluções de DNS e usa modelos ML específicos para revelar se a classificação pode ser disseminada de vértices de domínio maliciosos e de phishing para as imediações do gráfico. Treinado com milhões de domínios, o modelo impede milhões de cliques em links de phishing anualmente.

Se a ameaça não for detida antes da execução, a segunda camada de proteção é acionada. O mecanismo de detecção comportamental monitora todos os comportamentos de processos usando um modelo de IA comportamental, a capacidade do KSN e informações de análises estáticas para detectar padrões maliciosos e deter comportamento malicioso.

E isso não é tudo. Mesmo se uma ameaça conseguir penetrar a camada de análise estática, a próxima camada é acionada: soluções de segurança altamente especializadas para clients SOC especializados. O Kaspersky Next XDR tira proveito da IA para aprimorar a eficácia das equipes de SOC ao reduzir o ruído dos alertas supérfluos, analisando automaticamente e esclarecendo eventos, além de detectar comportamento malicioso como ataques de sequestro de DLL. O Kaspersky Threat Intelligence Portal usa IA para resumir dados de inteligência contra ameaças e reduzir a carga de trabalho dos analistas.

Como descrito acima, a Kaspersky tira proveito da ML em divesas camadas, desde a análise de estrutura de arquivo até o monitoramento de comportamento, usando diversos tipos de IA. A tecnologia engloba cenários em dispositivos e também baseados na nuvem, como por exemplo o impulso de gradiente, redes neurais profundas e grandes modelos de linguagem. Essas tecnologias fornece proteção a milhões de usuários em tempo real, adaptando-se à evolução dinâmica da criminalidade cibernética.

Ao cultivar o poder da IA, a Kaspersky vai muito além da detecção de malware conhecido, prevendo e neutralizando ameaças emergentes com uma precisão imbatível.[1] Essa abordagem proativa garante que usuários sejam protegidos contra ataques sofisticados, como exploits de dia zero e malware polimórfico, que evoluem constantemente para burlar os sistemas de detecção.

Além disso, as soluções Kaspersky orientadas por IA são projetadas para minimizar a quantidade de falsos positivos, equilibrando segurança robusta com eficiência operacional. Graças às atualizações e aprendizagem contínua, os sistemas se adaptam a novos vetores de ataque e cenários de ameaças, mantendo um alto nível de precisão e confiabilidade. Seja protegendo dispositivos de usuários, redes corporativas ou infraestrutura crítica, as tecnologias ML capacitam usuários a se manterem sempre à frente dos cibercriminosos.

1 Kaspersky. A mais testada. A mais premiada. Proteção Kaspersky (Kaspersky, 2024).

Sobre a Kaspersky

A Kaspersky é uma empresa global de cibersegurança e privacidade digital fundada em 1997. Com mais de um bilhão de dispositivos protegidos contra ameaças cibernéticas emergentes e ataques direcionados, a inteligência de ameaças profunda e o expertise em segurança da Kaspersky estão constantemente se transformando em soluções e serviços inovadores para proteger empresas, infraestrutura crítica, governos e consumidores em todo o mundo. O portfólio de segurança abrangente da empresa inclui proteção de endpoint líder, produtos e serviços de segurança especializados e soluções de imunidade cibernética para combater ameaças digitais sofisticadas e em constante evolução. Ajudamos mais de 200.000 clientes corporativos a proteger o que mais importa para eles. Saiba mais em www.kaspersky.com.br.

www.kaspersky.com.br