Kaspersky Threat Data Feeds

kaspersky BRING ON THE FUTURE

Kaspersky Threat Data Feeds

Kaspersky Threat Data Feeds

Ciberataques acontecem todos os dias. As ameaças virtuais estão em constante crescimento em termos de frequência, complexidade e ocultação, à medida que tentam comprometer as defesas de suas vítimas. Os criminosos utilizam cadeias de kill chain, campanhas e táticas, técnicas e procedimentos (TTPs) personalizados de intrusão para interromper seus negócios ou causar danos aos seus clientes. É bem evidente que a proteção de cibersegurança exige novos métodos, baseados em inteligência de ameaças.

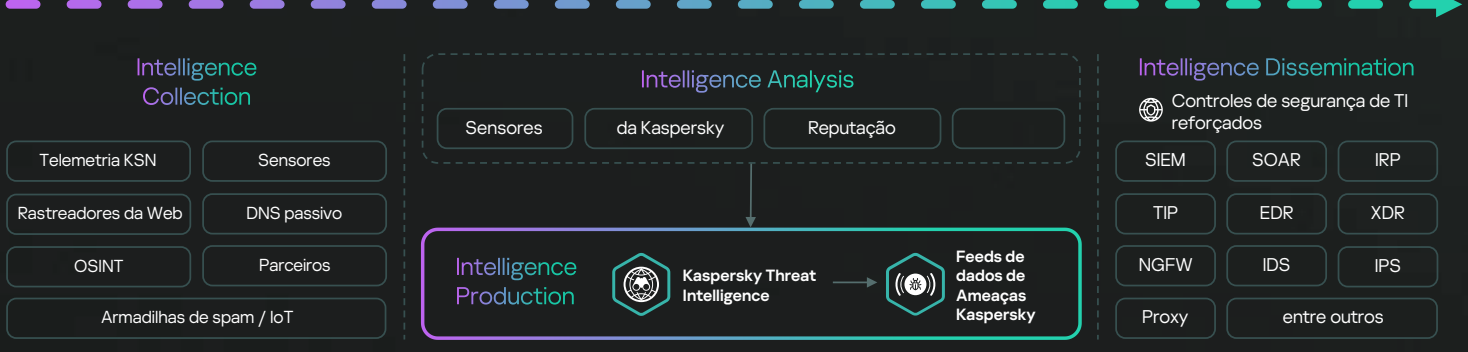
Ao integrar feeds de inteligência de ameaças sempre atualizados contendo informação sobre IPs, URLs e hashes de arquivos suspeitos e perigosos nos sistemas de segurança existentes, como SIEM, SOAR e plataformas de inteligência de ameaças, as equipes de segurança podem automatizar o processo de triagem de alertas inicial, fornecendo simultaneamente aos seus especialistas em triagem contexto suficiente para identificar imediatamente alertas que devem ser investigados ou encaminhados para equipes de resposta a incidentes para investigação e resposta adicionais.

Dados contextuais

As entradas de feeds fornecidos pela Kaspersky contêm dados contextuais que ajudam você a confirmar e priorizar ameaças com agilidade:

- Nomes de ameaças
- Endereços de IP e nomes de domínio de recursos maliciosos da Web
- Hashes de arquivos maliciosos
- Objetos vulneráveis e comprometidos
- Táticas, técnicas e procedimentos de ataques segundo a classificação MITRE AT&CK
- Marcação de data e hora
- Geolocalização
- Popularidade, e assim por diante...

Como funciona



Os feeds de dados de ameaças da Kaspersky são agregados a partir de fontes fundidas, heterogêneas e altamente confiáveis da Kaspersky:

Kaspersky SecurityNetwork

Infraestrutura de nuvem sofisticada que coleta e analisa dados anônimos de ameaças cibernéticas de mais de 400 milhões de participantes voluntários em todo o mundo para fornecer a resposta mais rápida às novas ameaças, aproveitando a análise de big data, aprendizado de máquina e expertise humana.

Rastreadores da Web

Coletar novas amostras de malware e legítimas de diversas fontes: OSINT, pesquisa realizada por analistas da Kaspersky e nossos próprios sistemas de processamento e análise automática que extraem URLs de malware.

BotFarms

Uma equipe de pesquisa dedicada a botnets extrai configurações de bots, faz engenharia reversa de seus protocolos de comunicação e monitora comandos dos centros de comando para obter inteligência de ameaças valiosa.

Armadilhas de spam

Todo ano, nossos sistemas anti-phishing impedem mais de 500 milhões de cliques em links de phishing e mais de 160 milhões de anexos de e-mail maliciosos, dos quais extraímos dados adicionais para enriquecer nossos fluxos de dados.

Parceiros

Nós participamos de parcerias para compartilhar amostras maliciosas com outros fornecedores e organizações de cibersegurança.

Sensores

Honeypots, sinkholes e outros métodos de interceptar ataques ITW. Por exemplo (incluindo dispositivos IoT, sistemas vulneráveis, software etc). Os analistas da Kaspersky pesquisam tentativas de ataque e métodos dos atacantes, extraem indicadores de comprometimento e os vinculam a outras fontes de dados.

DNS passivo

Os dados são coletados globalmente por meio de terceiros confiáveis, como organizações de hospedagem e provedores de serviços de internet.

OSINT

Os dados do adversário são coletados automaticamente de fontes publicamente disponíveis, como veículos de notícias, mídias sociais, relatórios públicos, dark web etc. Usamos esses dados para buscar novas amostras maliciosas explorando a infraestrutura do adversário, continuamente adicionando ao nosso banco de conhecimento.

Cada indicador detectado passa por um processo de triagem em várias etapas em um sistema de processamento automatizado que utiliza tecnologias de confiança e reputação e modelos de aprendizado de máquina treinados em amostras de centenas de milhões de arquivos confiáveis e maliciosos para eliminar falsos positivos. Cada indicador também é analisado em várias áreas de testes, das quais dezenas de atributos adicionais, como TTPs, comportamento de rede, comportamento do sistema operacional e uma série de outras relações, são extraídos.

Tudo isso transforma o Kaspersky Threat Intelligence em uma poderosa fonte de inteligência em nível tático que pode fortalecer seus centros de monitoramento de ameaças e detectar adversários na linha de frente de sua organização.

Destaques

Todos os feeds são automaticamente gerados em tempo real com base em descobertas em todo o mundo, fornecendo altos índices de detecção e precisão.

Documentações adicionais, amostras, um gerente de conta técnico dedicado e suporte técnico da Kaspersky combinam-se para permitir uma integração direta.

Formatos de disseminação leves e simples (JSON, CSV, OpenIoC, STIX) por meio de HTTPS, TAXII ou mecanismos de ad-hoc delivery, suportam fácil integração de feeds em soluções de segurança Principais SIEMs e plataformas de TI são totalmente suportados.

Feeds de dados repletos de falsos positivos não têm valor, por isso, são aplicados testes e filtros muito extensos antes de lançar os feeds, para garantir que 100% dos dados verificados sejam entregues

Centenas de especialistas, incluindo analistas de segurança de todo o mundo, especialistas em cibersegurança renomados das equipes GReAT e R&D contribuem para gerar esses feeds. Os agentes de segurança recebem informações críticas e alertas gerados a partir de dados da mais alta qualidade, sem correr o risco de serem inundados por indicadores e avisos excessivos

Todos os feeds são gerados e monitorados por uma infraestrutura altamente tolerante a falhas, assegurando disponibilidade contínua.

Benefícios

1. Reforce suas soluções de defesa de rede, incluindo SIEMs, firewalls, IPS/IDS, proxy de segurança, soluções de DNS, anti-APT, com indicadores de comprometimento (IOCs) atualizados continuamente, e contexto acionável para fornecer insights sobre ciberataques e uma maior compreensão da intenção, das capacidades e dos alvos dos seus adversários.

2. Melhore e acelere sua resposta a incidentes e recursos forenses automatizando o processo de triagem inicial e fornecendo aos seus analistas de segurança contexto suficiente para identificar imediatamente os alertas que precisam ser investigados ou escalados para equipes de resposta a incidentes para qualquer investigação e resposta adicionais.

3. Impeça o roubo de materiais confidenciais e propriedade intelectual de máquinas infectadas para fora da organização. Detecte materiais infectados rapidamente para proteger a reputação da sua marca, mantenha sua vantagem competitiva e garanta oportunidades de negócios.

4. Como um MSSP, expanda seus negócios fornecendo uma inteligência de ameaças líder no setor como serviço premium para seus clientes.

5. Como uma CERT, melhore e expanda suas capacidades de detecção e identificação de ciberameaças.

Kaspersky Threat Intelligence

Kaspersky Threat Intelligence fornece acesso a uma ampla gama de informações coletadas por nossos analistas e pesquisadores de classe mundial. Esses dados ajudarão sua organização a combater efetivamente as ameaças cibernéticas de hoje.

Nossa empresa possui um profundo conhecimento, ampla experiência em pesquisa de ameaças cibernéticas e insights exclusivos em todos os aspectos da cibersegurança, fornecendo inteligência de ameaças táticas, operacionais e estratégicas atualizadas.
Isso nos tornou um parceiro confiável de órgãos de segurança e governamentais ao redor do mundo, incluindo a Interpol e várias unidades de CERT. E tudo isso está disponível para você como dados relevantes e acionáveis por meio do Portal do Kaspersky Threat Intelligence.

Kaspersky Threat Intelligence

Saiba mais

www.kaspersky.com.br

#kaspersky
#bringonthefuture