Kaspersky Research Sandbox

Kaspersky Threat Attribution Engine

Análise de similaridades Kaspersky

Kaspersky Threat Analysis

kaspersky bring on the future

Kaspersky Threat Analysis

Kaspersky Threat Analysis

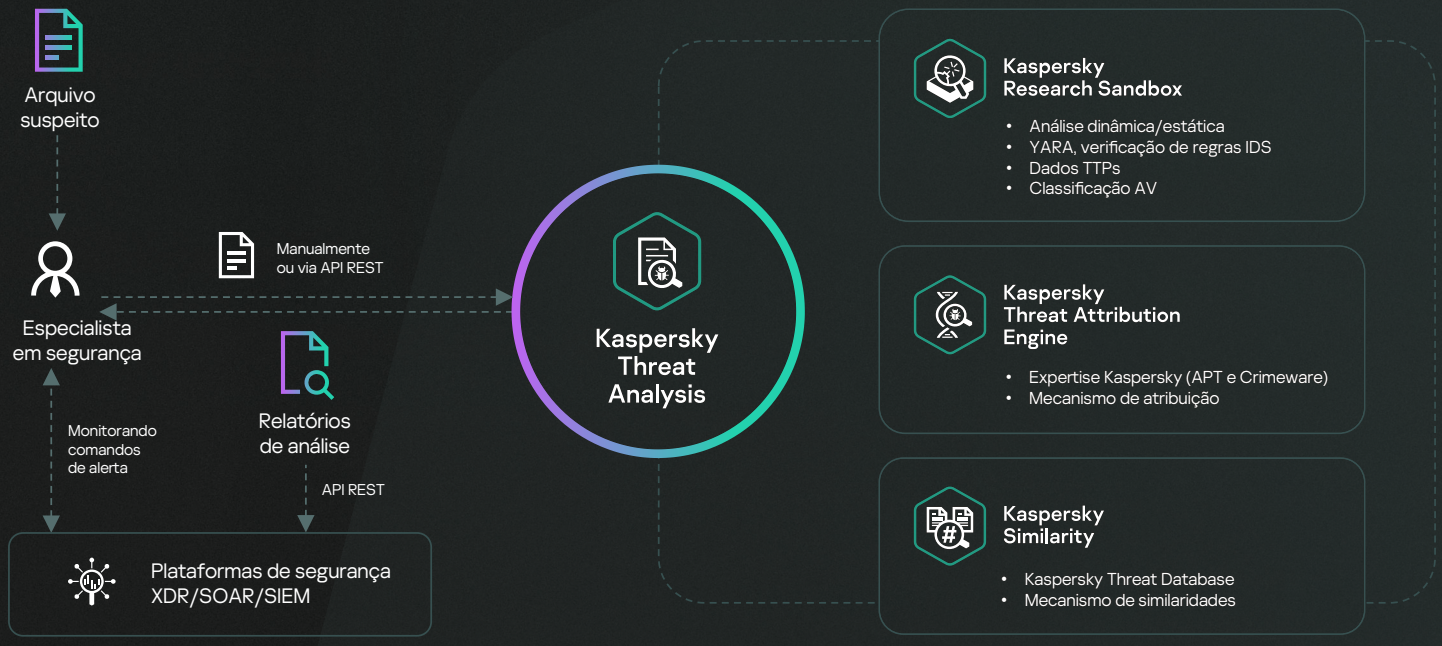
Diante de uma ciberameaça em potencial, suas decisões e sua capacidade de ação podem ser ambos cruciais. É impossível prever todos os ataques direcionados da atualidade usando apenas ferramentas de antivírus tradicionais. Mecanismos antivírus conseguem deter apenas as ameaças conhecidas e suas variantes, enquanto agentes de ameaças sofisticados utilizam todos os meios à sua disposição para escapar da detecção automática. A quantidade de alertas de segurança processados pelos SOCs diariamente cresce exponencialmente. Com o volume de amostras de malware geradas diariamente, a priorização de alertas eficazes, triagem e validação se torna ainda mais inviável.

Combinar a inteligência contra ameaças, a análise dinâmica, a atribuição de ameaças e tecnologias de similaridade fornece uma ferramenta poderosa para detectar objetos maliciosos anteriormente despercebidos. Para ajudar os investigadores de segurança a se manterem informados sobre ameaças emergentes, a Kaspersky fornece uma estrutura única resiliente para automatizar a análise de rotina de arquivos suspeitos.

Além da tecnologia de análise de ameaças tradicional como sandbox, o Kaspersky Threat Analysis fornece a você tecnologias de similaridade relacionadas e capacidade de atribuição de ponta. Essa é uma abordagem híbrida que proporciona uma análise de ameaças eficiente, para que você possa tomar decisões, dispondo de todas as informações para manter sua infraestrutura em segurança.

O Kaspersky Threat Analysis é fornecido via uma solução web unificada e também em interface RESTful, permitindo aos usuários definir parâmetros específicos para analisar objetos suspeitos com alta eficiência. Várias ferramentas de análise de ameaças combinadas vão permitir à sua equipe analisar a situação de todos os ângulos, fornecendo a você relatórios detalhados para responder de maneira ágil e eficaz.

Como funciona



Kaspersky
Threat Analysis

Kaspersky
Research
Sandbox

Tecnologias de sandbox

são ferramentas de análise dinâmica poderosas que permitem investigar origens de amostras de arquivos, coletar IOCs com base na análise comportamental e identificar objetos maliciosos não detectados por ferramentas tradicionais de antivírus.

Versões na nuvem e on-premise disponíveis.

Sandbox

O Kaspersky Research Sandbox foi desenvolvido diretamente em nosso complexo de sandboxing em laboratório, uma tecnologia que está evoluindo há décadas. A solução incorpora todo o conhecimento sobre comportamentos de malware, adquiridos graças à nossa constante pesquisa sobre ameaças, possibilitando a detecção de mais de 420 mil novos objetos maliciosos diariamente. Você conta com uma abordagem híbrida, combinando análise comportamental e técnicas anti-evasão, com tecnologias de simulação humana.

Implementada localmente, essa nova tecnologia avançada também evita a exposição de dados fora do perímetro da organização. O Kaspersky Research Sandbox on-premise também permite criar ambientes de execução personalizados, adaptado para ambientes reais, o que aumenta a precisão da detecção de ameaças e a velocidade de investigação.

Vantagens da solução

Arquivos suspeitos, não detectados por ferramentas de antivírus, podem revelar traços maliciosos apenas pelo seu comportamento. O Kaspersky Research Sandbox permite emular o comportamento e destacar ações perigosas.

Destaques do produto

Análise de objetos automatizada em ambientes Windows, Linux e Android

Imagens personalizadas permitem análise de ameaças em sistemas operacionais Windows e aplicativos (somente os que se aplicam a ambientes reais)

A pontuação de ameaças com base em métricas e dados obtidos durante a execução de arquivos mostra o nível de perigo do objeto analisado

Técnicas anti-evasão avançadas e tecnologias de simulação humana

Upload manual de amostras e API REST aprimorada para integração com fluxos de trabalho automatizados

Suporte à análise de mais de 200 tipos de arquivos com relatórios de análise detalhados

Regras Suricata personalizadas para verificar tráfego de rede podem ser adicionadas e usadas com outras regras

+1000 caças únicas para extração de TTPs pela MITRE ATT&CK

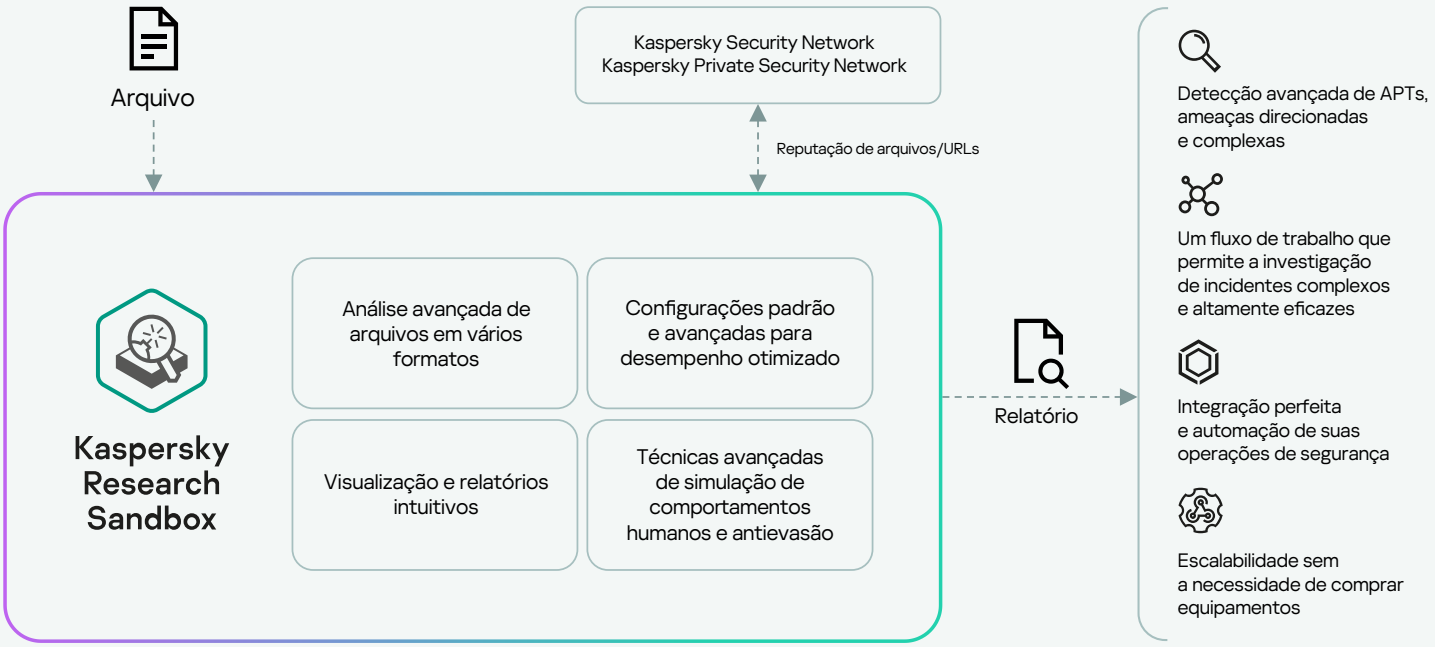
Suporte de modo interativo (aguardado para Q1 de 2024)

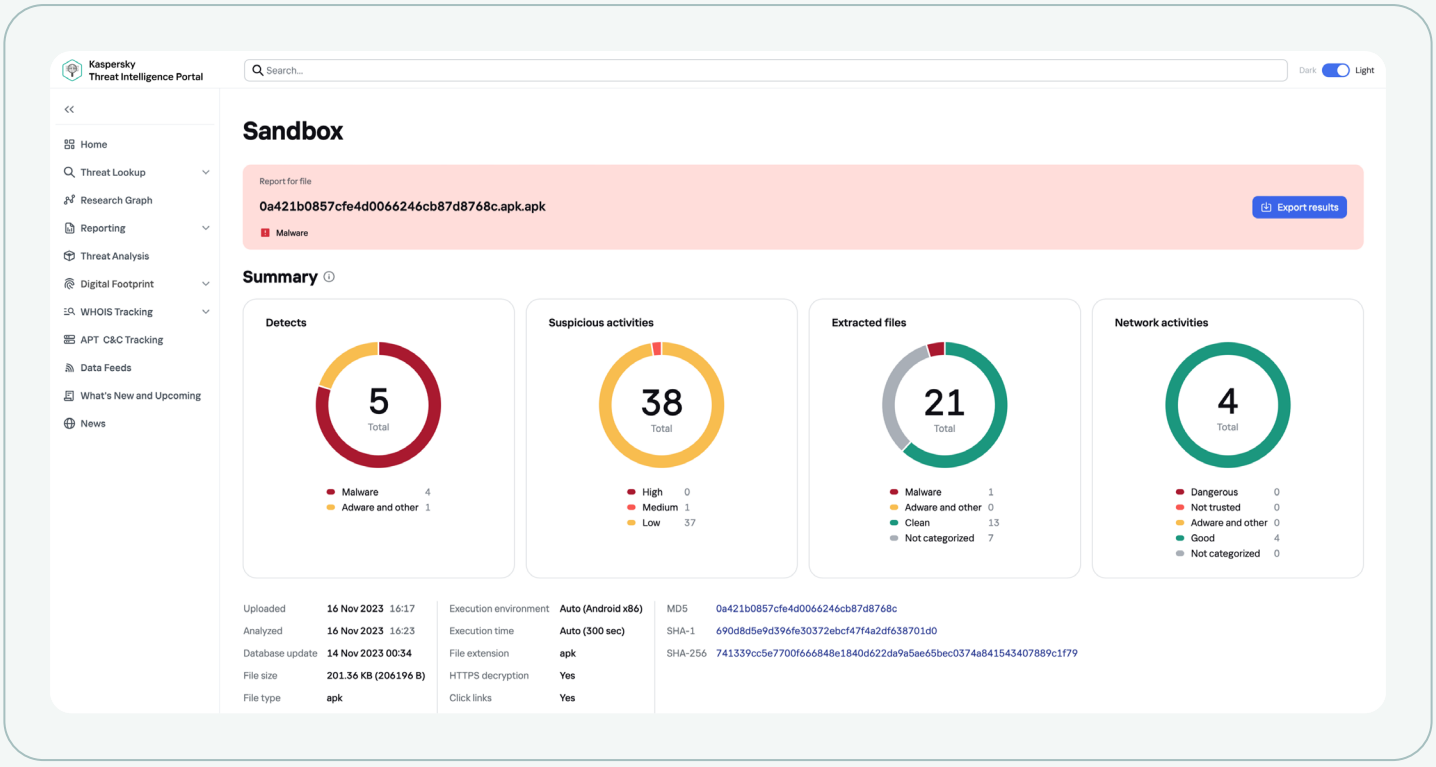
O produto é compatível com implantações bare metal. A configuração de hardware depende do desempenho necessário e pode ser dimensionada. É necessária no mínimo uma conexão ISP (duas ou mais são recomendadas para a tolerância a falhas), 100 Mbps por canal.

O Kaspersky Research Sandbox é baseado em tecnologia proprietária patenteada (número da patente US10339301). Ao criar as condições exatas que acionam a execução do malware, a solução permite que pesquisadores analisem arquivos/URLs suspeitos em uma única tentativa.

Para evitar exposição, um arquivo mal-intencionado pode primeiro investigar se ele está em uma máquina virtual ou permanecer inativo até que a sandbox não esteja mais operando. Em tais casos, a tecnologia patenteada agiliza o fluxo de tempo na máquina virtual para que o código malicioso seja forçado a antecipar sua execução.

Esquema de operação de alto nível do Kaspersky Research Sandbox





Relatórios de análise detalhados

Após a conclusão da análise, o Research Sandbox fornece um relatório detalhado sobre o comportamento e a funcionalidade da amostra analisada, permitindo que você defina os procedimentos de resposta apropriados:

Resumo	Informações gerais sobre os resultados da execução de um arquivo/navegação em um URL.
Nomes das detecções	Uma lista de detecções (tanto do antivírus quanto comportamentais) registradas durante a execução do arquivo.
Regras de rede acionadas	Uma lista de regras Suricata de rede acionadas durante a análise do tráfego do objeto executado.
Mapa de execução	Uma sequência de atividades do objeto representada graficamente e o relacionamento entre elas.
Atividades suspeitas	Atividades suspeitas – uma lista de atividades suspeitas registradas.
Capturas de Tela	Um conjunto de capturas de tela obtidas durante a execução do arquivo/navegação no URL.
Imagens PE carregadas	Uma lista de imagens PE carregadas detectadas durante a execução do arquivo/navegação no URL.
Operações de arquivo	Uma lista de operações registradas durante a execução do arquivo/navegação no URL.
Operações do Registro	Uma lista de operações executadas no Registro do sistema operacional detectadas durante a execução do arquivo/navegação no URL.
Operações de processos	Uma lista de interações do arquivo com vários processos registradas durante a execução do arquivo.
Operações de sincronização	Uma lista de operações de objetos de sincronização criados (mutex, evento, semáforo) que foram registradas durante a execução do arquivo/navegação no URL.
Arquivos baixados	Uma lista de arquivos extraídos do tráfego de rede durante a execução do arquivo/navegação no URL.
Arquivos descartados	Uma lista de arquivos salvos (criados ou modificados) pelo arquivo executado.
HTTPS/HTTP/DNS/IP/TCP/UDP e etc.	Detalhes de sessões/solicitações de rede registradas durante a execução do arquivo/navegação no URL
Despejo do tráfego de rede (PCAP)	A atividade da rede pode ser exportada no formato PCAP
Matriz MITRE ATT&CK	Todas as atividades de processos identificadas e gravadas durante a emulação são apresentadas na forma de uma matriz MITRE ATT&CK.

Kaspersky
Threat Analysis

Kaspersky
Threat Attribution
Engine

Atribuição de ameaças

A tarefa de rastrear, analisar, interpretar e reduzir as ameaças de segurança de TI em constante evolução é altamente desafiadora. Deixando de lado todo a fama recém adquirida, a inteligência contra ameaças tem um valor real e a atribuição de ameaças é um elemento essencial nesse caso.

Versões na nuvem e on-premise disponíveis.

Atribuição

O Kaspersky Threat Attribution Engine é uma ferramenta única de análise de ameaças, que fornece insights sobre a origem de malwares de alto nível e seus possíveis agentes. A solução conecta rapidamente um arquivo suspeito a ameaças APT, agentes e campanhas conhecidos, usando um algoritmo exclusivo e bancos de dados especiais compreendendo amostras de malware APT e a coleta mais ampla do mercado para arquivos limpos, extraídos por especialistas Kaspersky durante mais de 25 anos.

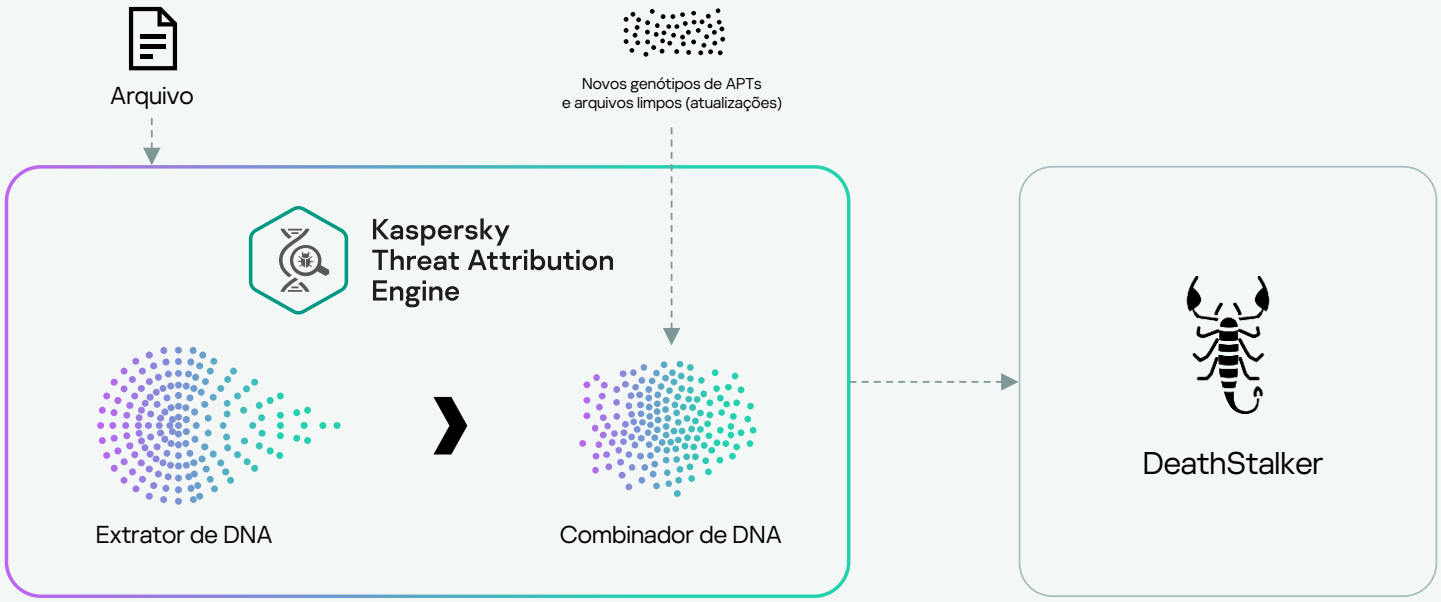
Rastreamos mais de 1.100 agentes e campanhas de ameaças e lançamos mais de 200 relatórios de inteligência de ameaças por ano. A pesquisa contínua apoia a coleta de APTs, contendo mais de 80 mil arquivos que, em conjunto com o uso de ferramentas automatizadas, resulta em níveis altamente precisos de atribuição.

O produto oferece uma abordagem exclusiva para comparar amostras semelhantes, garantindo taxas de falsos positivos quase nulas. Qualquer novo ataque pode ser rapidamente vinculado a um malware APT, a ataques direcionados anteriores e grupos de hackers, o que ajuda a identificar a ameaça de maior risco dentre incidentes menos importantes, além de permitir a tomada de medidas protetivas em tempo hábil para evitar que um invasor tenha acesso ao sistema. O Kaspersky Threat Attribution Engine pode ser implementado em um ambiente seguro de modo a restringir o acesso de terceiros às informações processadas e objetos enviados.

Vantagens da solução

Atribuição de uma arquivo a um determinado agente de ameaça, juntamente com o conhecimento do agente de ameaça, permite saber a origem da amostra na cyber kill chain, específica para tal risco. Por sua vez, fornece o conhecimento sobre onde buscar por outros IoCs/IoAs e como deter todo o ataque, em vez de bloquear apenas um arquivo em particular.

Esquema de operação de alto nível do Kaspersky Threat Attribution Engine



Destaques do produto

Fornece acesso imediato a um repositório de dados selecionados sobre milhares de agentes e amostras de APT e outras ameaças (usando o mecanismo antivírus)

Insights exclusivos sobre campanhas de alta repercussão (+400), investigadas por especialistas Kaspersky

Permite a priorização eficiente de ameaças manuais ou automatizadas e triagem de alertas

Funcionalidade para adicionar amostras e agentes privados, instruindo o produto para detectar amostras que sejam semelhantes aos arquivos em suas coleções particulares.

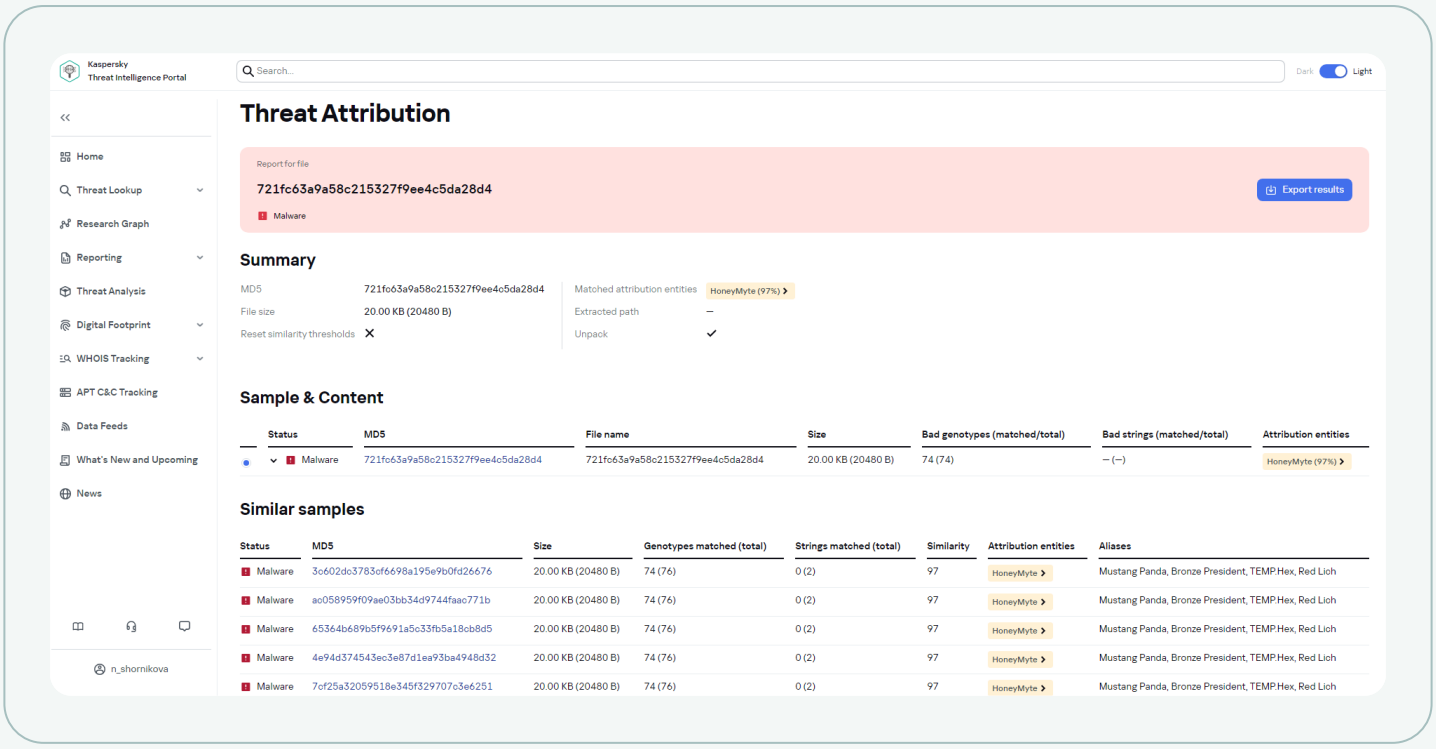
Upload manual de amostras e API REST aprimorada para integração com fluxos de trabalho automatizados

Oferece suporte à implementação em infraestruturas na nuvem, como Amazon Web Services (AWS), permitindo configuração rápida do produto e economia de custos, pois não há necessidade de investir antecipadamente em hardware

Exportação para regras YARA para pesquisa/verificação automatizada adicional de arquivos semelhantes ou integração com soluções terceirizadas

Exportação para o formato STIX 2.1 (os formatos TXT e JSON também são suportados) para análise automatizada adicional de logs de segurança ou integração com soluções/controles de segurança terceirizados

Funcionalidade para descompactar arquivos protegidos por senha com senhas personalizadas



Método de busca proprietário

Para vincular um malware a entidades de atribuição, o Kaspersky Threat Attribution Engine usa um método próprio exclusivo para buscar genótipos semelhantes entre arquivos. O método envolve:

Análise genética de amostras

ao extrair os seguintes elementos do código:

- Genótipos — blocos distintos de código binário
- Strings — strings distintas de caracteres

Busca automática de arquivos analisados

por genótipos e strings semelhantes a genótipos e strings de amostras APT previamente analisadas ou já vinculadas a entidades de atribuição.

Basedo em genótipos e strings semelhantes

encontrados em amostras APT, fornecendo um relatório sobre a origem da amostra analisada, entidades de atribuição relacionadas e quaisquer semelhanças entre esta amostra e amostras APT conhecidas.

Kaspersky
Threat Analysis

Kaspersky
Similarity

Similaridade de arquivos

Para criar uma linha de defesa robusta, nem sempre é necessário ver o inimigo. O Kaspersky Similarity identifica amostras de arquivos com funções semelhantes e proteja-se contra ameaças evasivas e desconhecidas.

Versão na nuvem disponível via Kaspersky Threat Intelligence Portal.

Similaridade

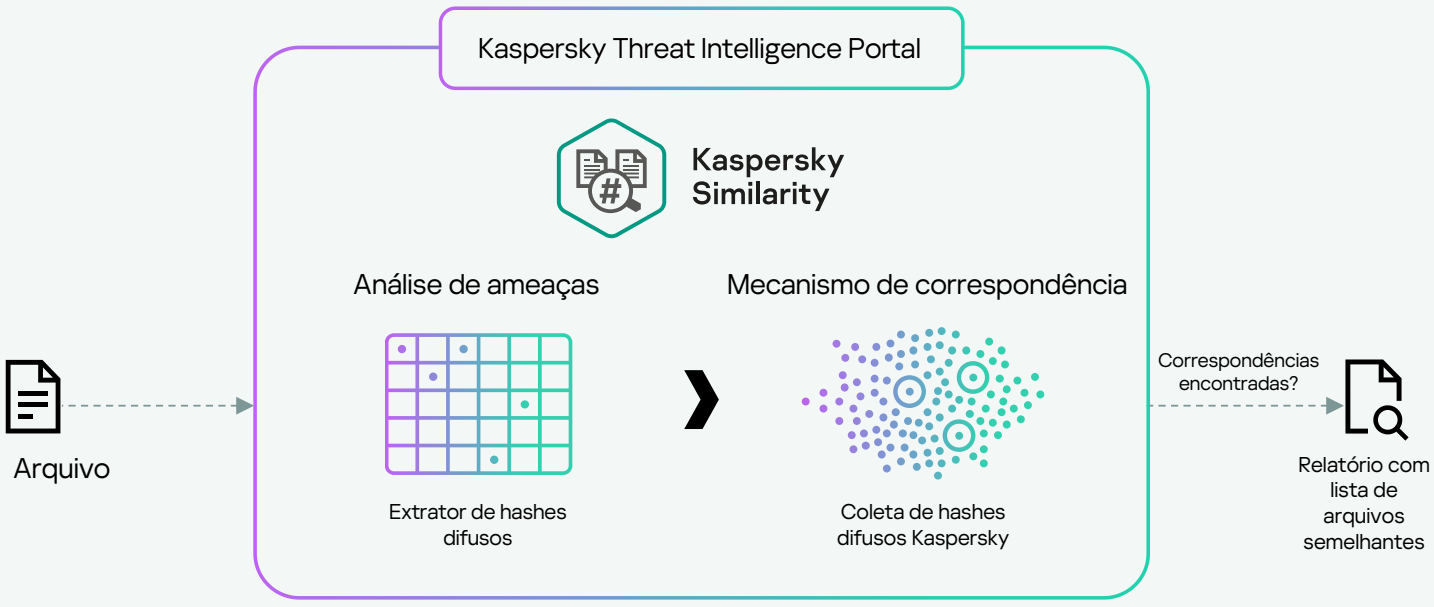
Kaspersky Similarity é um recurso adicional disponível via Threat Intelligence Portal para ambos os usuários do Kaspersky Research Sandbox e do Kaspersky Threat Attribution Engine. A solução ajuda a identificar arquivos com aparência e comportamento semelhantes.

Arquivos semelhantes são buscados e calculados em relação ao arquivo original, usando tecnologia de ponta, desenvolvida pelos especialistas Kaspersky, com base em mais de 50 tipos de hashes de similaridade únicos. Isso permite garantir a precisão e alta fidelidade dos resultados de similaridade.

Vantagens da solução

Encontre malware semelhantes (evasivos) e busque pela infraestrutura, para ter certeza que qualquer ligeira modificação na amostra feita pelos criminosos não escapará do seu radar. A tecnologia é diferente da atribuição: mesmo arquivos de malware semelhante não atribuído podem ser encontrados.

Esquema de operação de alto nível do Kaspersky Similiarity



Relatórios de similaridade

Cada arquivo tem um formato, empacotadores de usuários, seções, strings, tabelas de importação específicas etc. Os especialistas Kaspersky criaram um conjunto de hashes para determinar a similaridade entre diferentes arquivos, com base nesses atributos. O Kaspersky Similarity permite aos usuários enviar um arquivo suspeito, extrair os hashes difusos e compará-los àqueles de arquivos do banco de dados de ameaças da Kaspersky. No caso de uma correspondência ser identificada, a solução gera uma lista de hashes para os principais arquivos maliciosos semelhantes e já conhecidos da Kaspersky, classificados por uma pontuação de similaridade. O relatório contém contexto adicional, com metadados para cada arquivo similar encontrado:

- Grau de confiança de similaridade
- Status do arquivo (malware, adware ou outro)
- Nome da ameaça
- Carimbos de hora da primeira e última detecção
- Quantidade de ocorrências (detecções)
- Hash de arquivos
- Tipo de arquivo
- Tamanho do arquivo

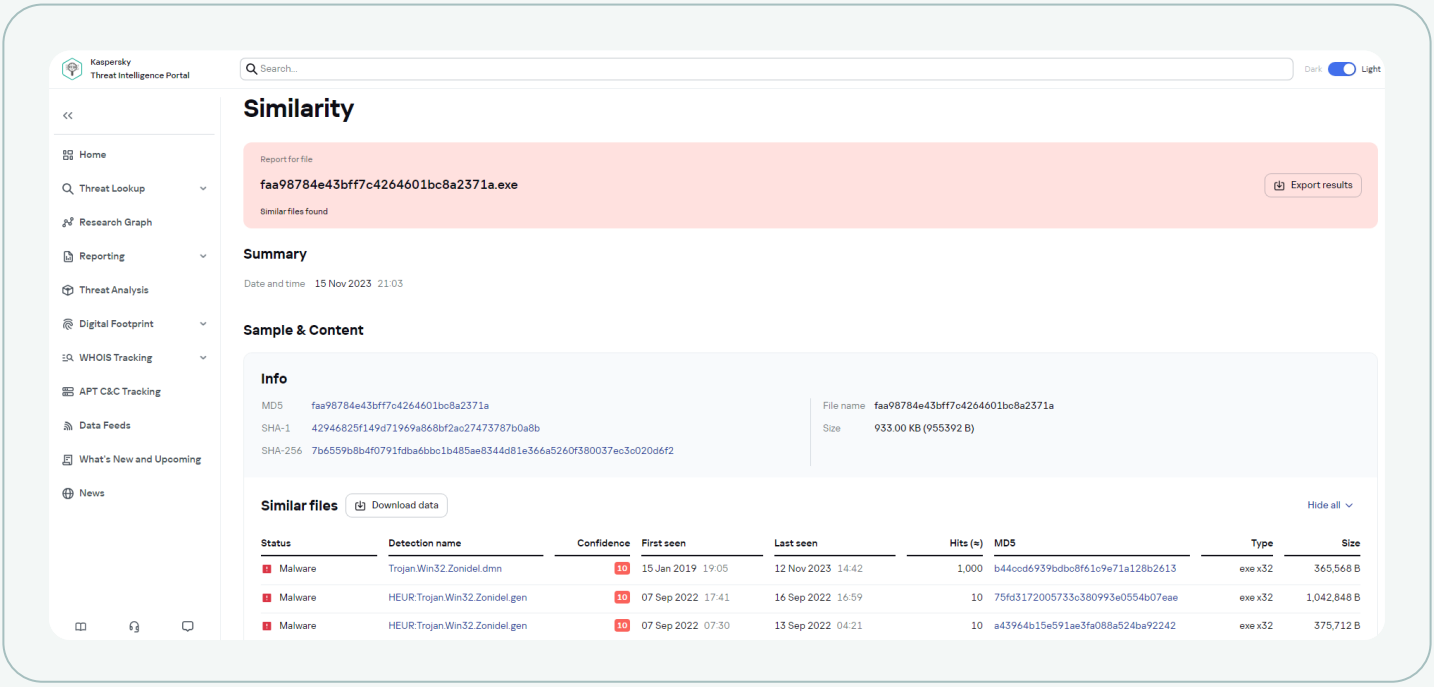
Destaques do recurso

A solução tira proveito do maior banco de dados de arquivos limpos e maliciosos do mercado, coletados ao longo de mais de 25 anos de experiência, permitindo a mais ampla cobertura para uma alta precisão de comparação.

Upload manual de amostras e API REST aprimorada para integração com fluxos de trabalho automatizados

Fornecido aos usuários do Kaspersky Research Sandbox e Kaspersky Threat Attribution gratuitamente, para aprimorar a eficácia das tecnologias e fornecer informações ambrangentes sobre o arquivo analisado.

A solução já é amplamente usada pelos especialistas Kaspersky para explorar novas ameaças e fornecer uma alta proteção nos nossos produtos, regularmente comprovada pelas altas taxas de avaliação positivas em testes independentes:



Casos de uso do Kaspersky Threat Analysis

O Kaspersky Threat Analysis fornece instrumentos experientes para detecção de ameaças desconhecidas que podem ser amplamente aplicados nos seguintes cenários:

Incident Response

Descoberta de ameaças evasivas

Análise estática/dinâmica de arquivos suspeitos

Descoberta de relações de um novo malware com determinado agente de ameaça, para revelar possíveis desdobramentos de ataques

Busca de ameaças

Verificação da infraestrutura para IoCs via relatórios

Detecção de modificações potencialmente maliciosas em arquivos limpos conhecidos

Identificação de IoCs compartilhados entre arquivos maliciosos conhecidos e desconhecidos

Análise de malware

Análise de ameaças desconhecidas

Identificação de malware relacionado para ajudar na engenharia reversa de arquivos ofuscados

O Kaspersky Threat Analysis é uma ferramenta de pesquisa flexível, com componentes interconectados que permitem a avaliação abrangente e multicamadas de elementos suspeitos, permitindo a identificação e classificação de ataques avançados. A solução ajuda equipes SOC, investigadores de segurança e analistas de malware a se manterem informados sobre ameaças existentes e emergentes relacionadas a malware, permitindo-lhes priorizar rapidamente e lidar com ameaças críticas, além de remediá-las mais eficazmente.

Kaspersky Threat Analysis

Saiba mais

www.kaspersky.com.br

#kaspersky
#bringonthefuture