Esteja a frente de seus adversários

Kaspersky Threat Intelligence

kaspersky BRING ON THE FUTURE

Kaspersky Threat Intelligence

A solução de Threat Intelligence da Kaspersky oferece acesso às informações de que você precisa para mitigar ciberameaças, além de obter informações relevantes para você, fornecidas pela nossa equipe líder mundial de investigadores e analistas.

O conhecimento, a experiência e as informações detalhadas da Kaspersky sobre todos os aspectos da segurança virtual fizeram com que nos tornássemos o parceiro de confiança das principais autoridades policiais e governamentais do mundo, incluindo a INTERPOL e as principais CERTs. O Kaspersky Threat Intelligence oferece acesso instantâneo a inteligência de ameaças, tática, operacional e estratégica.

O Kaspersky Threat Intelligence oferece uma visão abrangente do cenário global de ameaças. A solução combina fontes de inteligência, feeds de dados sobre ameaças e pesquisas internas, tudo analisado pela nossa equipe de especialistas para fornecer insights acionáveis que ajudam as organizações a se protegerem contra as ciberameaças.

O Kaspersky Threat Intelligence capacita você a

Identificar e prevenir ameaças de forma proativa

O Kaspersky Threat Intelligence mantém você a par de tudo sobre as ameaças e vulnerabilidades mais recentes, permitindo adotar medidas proativas para proteger seus sistemas antes que ocorra um ataque.

Obter visibilidade sobre sua pegada digital

O Kaspersky Threat Intelligence fornece uma visão abrangente da sua pegada digital, incluindo todos seus bens digitais que podem estar vulneráveis a ataques ou a comprometimentos.

Aprimore seus recursos de detecção de ameaças

O Kaspersky Threat Intelligence ajuda a reforçar as suas soluções de segurança implementadas com a mais recente inteligência de ameaças, aprimorando sua capacidade de detectar e bloquear ameaças avançadas.

Melhorar sua resposta a incidentes

O Kaspersky Threat Intelligence fornece informações em tempo real sobre ameaças emergentes e indicadores de comprometimento. Assim, você pode responder a incidentes de forma rápida e eficaz.

Cumprir com os regulamentos e normas

Todas as empresas estão sujeitas a diversas regulamentações e normas do seu setor de atuação. O Kaspersky Threat Intelligence auxilia na conformidade, ajudando você a cumprir com esses requisitos.

Valorizar ainda mais seus especialistas internos

A equipe de especialistas Kaspersky conta com os pesquisadores mais experientes e respeitados do setor, que contribuem com uma gama de conhecimento e experiência para suas equipes de Segurança da Informação.

Feeds do Kaspersky Threat Data

Ciberataques acontecem todos os dias. As ciberameaças estão em constante evolução 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. Uma proteção eficaz exige novos métodos com inteligência de ameaças como base.

Ao integrar feeds de inteligência de ameaças que são atualizados constantemente - dos quais contém informações 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 categorização de alertas iniciais, fornecendo simultaneamente aos seus especialistas de triagem as informações necessárias para identificar imediatamente alertas que devem ser investigados ou encaminhados para equipes de resposta a incidentes para investigação e resposta adicionais.

O Kaspersky Threat Data Feed fornece informações de inteligência de ameaças em tempo real para ajudar você a proteger suas redes e sistemas contra ciberameaças. Os feeds de dados incluem informações sobre malwares conhecidos, sites de phishing, vulnerabilidades e exploits mais recentes, além de outros tipos de ciberameaças. Essas informações ajudam você a bloquear tráfego malicioso, manter seus softwares de segurança atualizados e adotar outras medidas para proteger-se contra ciberataques.

Dados Contextuais

Cada registro em cada feed de dados é enriquecido também com contextos acionáveis (nome das ameaças, data/hora, geolocalização, endereços de IP solucionados de recursos infectados da web, hashes, popularidade, e etc.). Os dados contextuais ajudam a mostrar um panorama geral para validação adicional e suporte na utilização dos dados. Após contextualizados, os dados podem ser usados diretamente para responder perguntas do tipo "quem, o que, onde e quando" para identificar seus adversários e ajudar você a agir o mais rápido possível.

Como funciona?

1

Os dados são coletados de uma variedade de fontes confiáveis, incluindo o Kaspersky Security Network e nossos próprios rastreadores, serviços de monitoramento contra ameaças de botnets (rastreamento 24 horas de botnets e seus alvos), armadilhas de spam, dados de grupos de pesquisa, parceiros e muito mais.

2

Todas as informações coletadas são cuidadosamente verificadas e tratadas em tempo real, usando vários métodos de pré-processamento: sandboxing, análise estatística e investigativa, ferramentas comparativas, perfil comportamental e análise de especialistas.

3

Os feeds de dados ajudam a coletar informações sobre ameaças sobre um alerta ou incidente e a aprofundar os detalhes. Também ajuda a responder às perguntas sobre "Quem? O que? Onde? Por que?" e identifique a origem dos ataques, permitindo uma tomada de decisão rápida para proteger sua empresa contra ameaças de qualquer complexidade.

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...

Benefícios do Kaspersky Threat Data Feeds

Melhore e acelere a resposta a incidentes e os recursos de análise investigativa

ao automatizar o processo de triagem inicial, 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.

Reforce suas soluções de segurança

ao incluir SIEMs, firewalls, IPS/IDS, proxy de segurança, soluções de DNS, anti-APT, com indicadores de comprometimento (IOCs) continuamente atualizados, e contexto acionável para fornecer insights sobre ciberataques e uma maior compreensão da intenção, capacidades e dos alvos de seus adversários. Suporte completo para os principais SIEMs (incluindo ArcSight, IBM QRadar, MS Sentinel, Splunk etc.) e plataformas de TI

Detenha ações de exfiltração de materiais confidenciais e propriedade intelectual

de máquinas infectadas para fora da sua organização. Detecte materiais infectados rapidamente para proteger a reputação da sua marca, mantenha sua vantagem competitiva e garanta oportunidades de negócios.

Expanda seus negócios de MSSP

ao fornecer inteligência de ameaças de ponta como um serviço premium para seus clientes. Como uma CERT, melhore e expanda suas capacidades de detecção e identificação de ciberameaças.

Kaspersky CyberTrace

O crescimento contínuo no número de feeds de dados de ameaças e fontes de inteligência de ameaças disponíveis torna difícil para as empresas determinar quais informações são realmente relevantes para elas. Ao mesmo tempo, a inteligência de ameaças é fornecida em diversos formatos e inclui muitos indicadores de comprometimento (IoCs), fazendo com que seja difícil para as SIEMs ou outros controles de segurança de rede assimilá-los.

Ao integrar inteligência de ameaças legível por máquina e atualizada em controles de segurança existentes, como sistemas de SIEM, os Centros de Operações de Segurança conseguem automatizar o processo de triagem inicial, fornecendo aos seus analistas de segurança contexto suficiente para identificar imediatamente alertas que precisam ser investigados ou escalados para as equipes de resposta a incidentes para investigação e resposta adicionais.

O Kaspersky CyberTrace é uma plataforma de inteligência contra ameaças que permite a integração perfeita de feeds de dados de ameaças com soluções de SIEM, para ajudar os analistas a aproveitar com mais eficácia a inteligência de ameaças nos fluxos de trabalho das operações de segurança existentes. Ele se integra a qualquer feed de inteligência de ameaças (seja da Kaspersky, de outros fornecedores, OSINT ou seus próprios feeds de clientes) nos formatos JSON, STIX, XML e CSV e oferece suporte à integração imediata com várias soluções de SIEM e fontes de log.

Instrumentos

O Kaspersky CyberTrace fornece um conjunto de instrumentos para operacionalizar a inteligência de ameaças de forma efetiva:

Um banco de dados de indicadores com pesquisa de texto completa e a capacidade de pesquisar usando consultas de pesquisa avançadas, permite pesquisas complexas em todos os campos de indicadores (incluindo campos de contexto).

As estatísticas de uso de feeds para medir a eficácia dos feeds integrados e da matriz de interseção de feeds ajudam a escolher os fornecedores de inteligência de ameaças mais valiosos

A marcação de IoCs simplifica o gerenciamento de IoC. Crie qualquer tag, especifique seu peso (importância) e use-a para a marcação manual de IoCs. Você também pode classificar e filtrar IoCs com base nessas tags e seus níveis de importância

O Gráfico de Pesquisa permite a você explorar visualmente os dados e as detecções armazenadas no CyberTrace e descobrir semelhanças entre as ameaças detectadas.

O recurso de exportação de indicadores permite a exportação de conjuntos de indicadores para controles de segurança, como listas de políticas (listas de bloqueios), além do compartilhamento de dados de ameaças entre instâncias do Kaspersky CyberTrace ou com outras plataformas de TI

Com o recurso de correlação histórica (retroscan), é possível analisar itens observáveis a partir de eventos verificados anteriormente usando os feeds mais recentes para encontrar ameaças previamente descobertas

O recurso multitenancy (multi-usuários) oferece suporte a MSSPs e casos de uso de grandes empresas

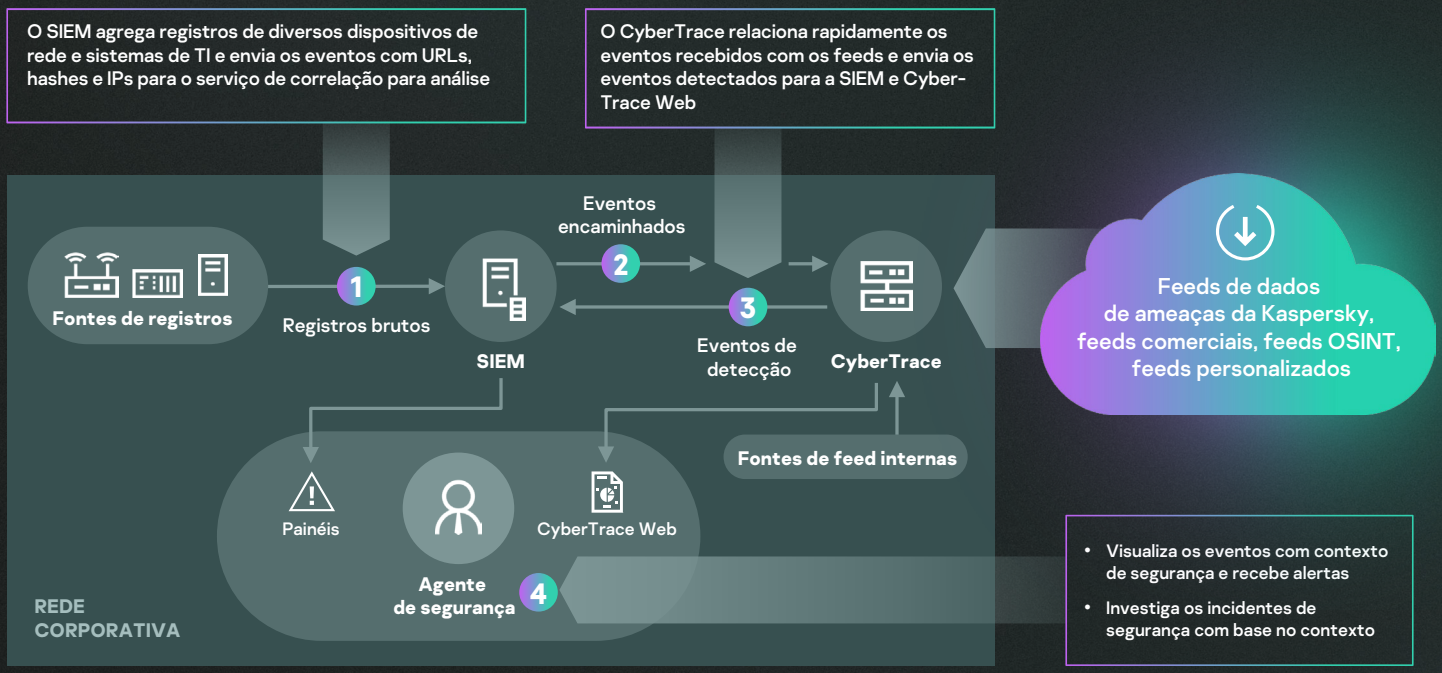
Um filtro envia eventos de detecção para soluções SIEM, reduzindo a carga sobre eles e também sobre os analistas

A HTTP RestAPI permite que você pesquise e gerencie a inteligência de ameaças

Páginas com informações detalhadas sobre cada indicador fornecem análises ainda mais profundas. Cada página apresenta todas as informações sobre um indicador de todos os fornecedores de inteligência de ameaças (desduplicação), de modo que os analistas podem discutir ameaças nos comentários e adicionar inteligência de ameaças internas sobre o indicador

A ferramenta usa um processo internalizado de análise e correspondência de dados recebidos, o que reduz significativamente a carga de trabalho do SIEM. O Kaspersky CyberTrace analisa logs e eventos recebidos, combina rapidamente os dados resultantes com os feeds e gera seus próprios alertas de detecção de ameaças.

Arquitetura



O Kaspersky CyberTrace e o Kaspersky Threat Data Feeds permitem aos analistas de segurança:

Filtrar e priorizar efetivamente grandes quantidades de alertas de segurança

Melhorar e acelerar os processos de triagem e de resposta inicial

Criar uma defesa proativa e orientada por inteligência

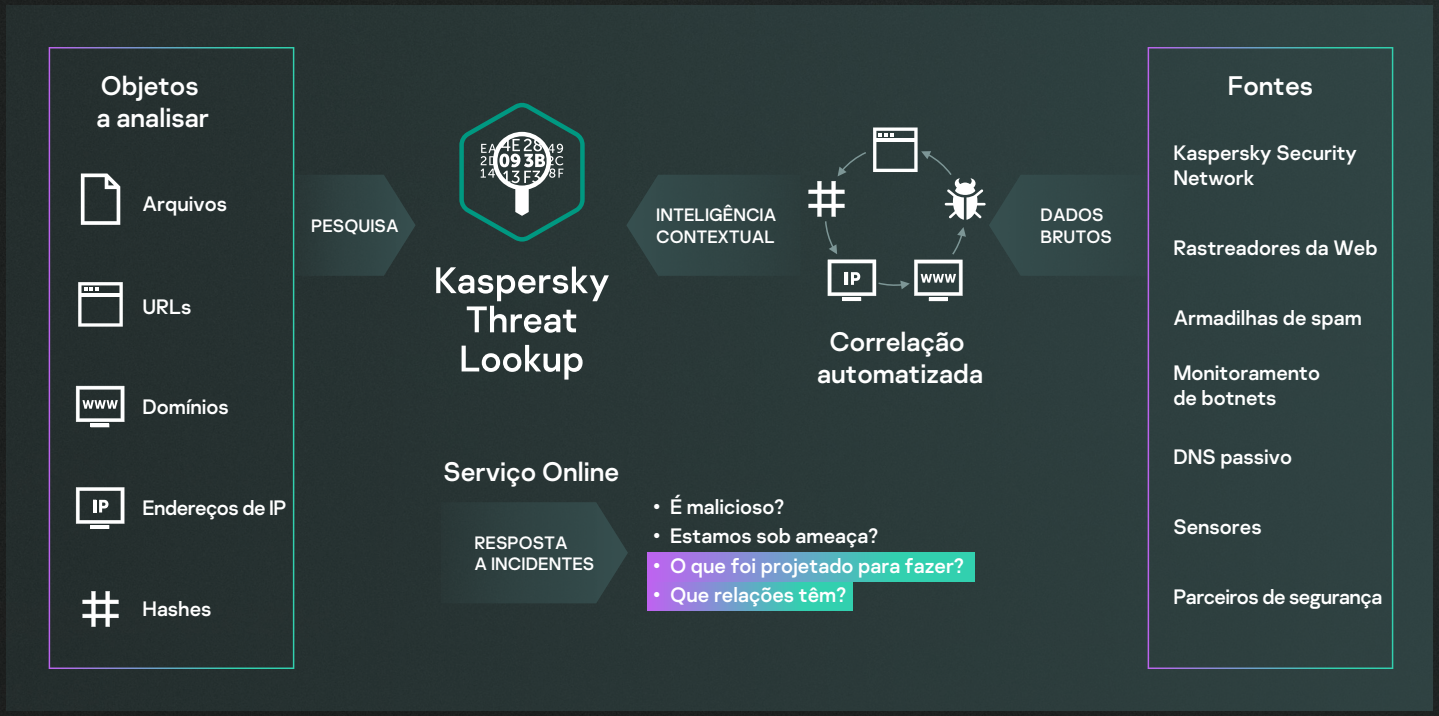
Identificar imediatamente alertas críticos para seus negócios e tomar decisões mais eficazes sobre os alertas que devem ser escalados para as equipes de IR

Kaspersky Threat Lookup

Os crimes virtuais não têm limites, e suas capacidades técnicas estão em constante evolução: os ataques estão cada vez mais sofisticados, pois os criminosos virtuais utilizam recursos da Dark Web para ameaçar seus alvos. As ciberameaças estão em constante crescimento em termos de frequência, complexidade e ocultação, à medida que novas tentativas são realizadas para comprometer as defesas de suas vítimas. Os invasores utilizam kill chains complicadas, e táticas, técnicas e procedimentos (TTP) personalizados nas campanhas para afetar suas operações, roubar seus dados ou causar danos aos seus clientes.

O Kaspersky Threat Lookup oferece todo o conhecimento adquirido pela Kaspersky sobre ciberameaças e como elas funcionam, reunindo tudo em um serviço da Web único e poderoso. O objetivo é fornecer às suas equipes de segurança o maior número de dados possível, prevenindo os ataques virtuais antes que afetem sua organização. A plataforma obtém a inteligência de ameaças detalhada mais recente sobre URL, domínios, endereços de IP, hashes de arquivos, nomes de ameaças, dados estatísticos/comportamentais, dados de WHOIS/DNS, atributos de arquivos, dados de geolocalização, cadeias de download, carimbos de data/hora, etc. O resultado é a visibilidade global de ameaças novas e emergentes, ajudando você a proteger a sua organização e a melhorar a resposta a incidentes.

Como funciona?



Destaques

Inteligência Confiável

Um atributo fundamental do Kaspersky Threat Lookup é a confiabilidade dos nossos dados de inteligência de ameaças, enriquecidos com contexto acionável. A Kaspersky é líder no campo dos testes Antimalware, demonstrando a qualidade inigualável da nossa inteligência de segurança ao fornecer as mais altas taxas de detecção, com quase zero falsos positivos

Busca de ameaças

Seja proativo na prevenção, detecção e resposta a ataques, para minimizar seu impacto e frequência. Rastreie e elimine eficientemente os ataques o mais cedo possível. Quanto mais cedo você descobrir uma ameaça, menos danos ela pode causar, mais rápido os reparos ocorrerão e mais cedo as operações de rede poderão voltar ao normal.

Facilidade de uso

Interface Web ou acesso à RESTful API Utilize o serviço no modo manual via uma interface da Web (usando um navegador web) ou acesse-o via uma API RESTful simples — o que você preferir

Uma gama de formatos de exportação

Exporte IOCs (indicadores de comprometimento) ou dados de contexto acionável para formatos de compartilhamento legíveis por máquina mais amplamente utilizados e organizados; como STIX, OpenIOC, JSON, Yara, Snort ou mesmo CSV, para extrair o máximo de benefícios da inteligência contra ameaças, automatizar o fluxo de trabalho das operações ou integrar em controles de segurança como SIEMs.

Benefícios do Kaspersky Threat Lookup

Conduza pesquisas profundas sobre indicadores de ameaças em um contexto altamente validado que permite priorizar ataques e focar na mitigação de ameaças que trazem maior risco ao seu negócio

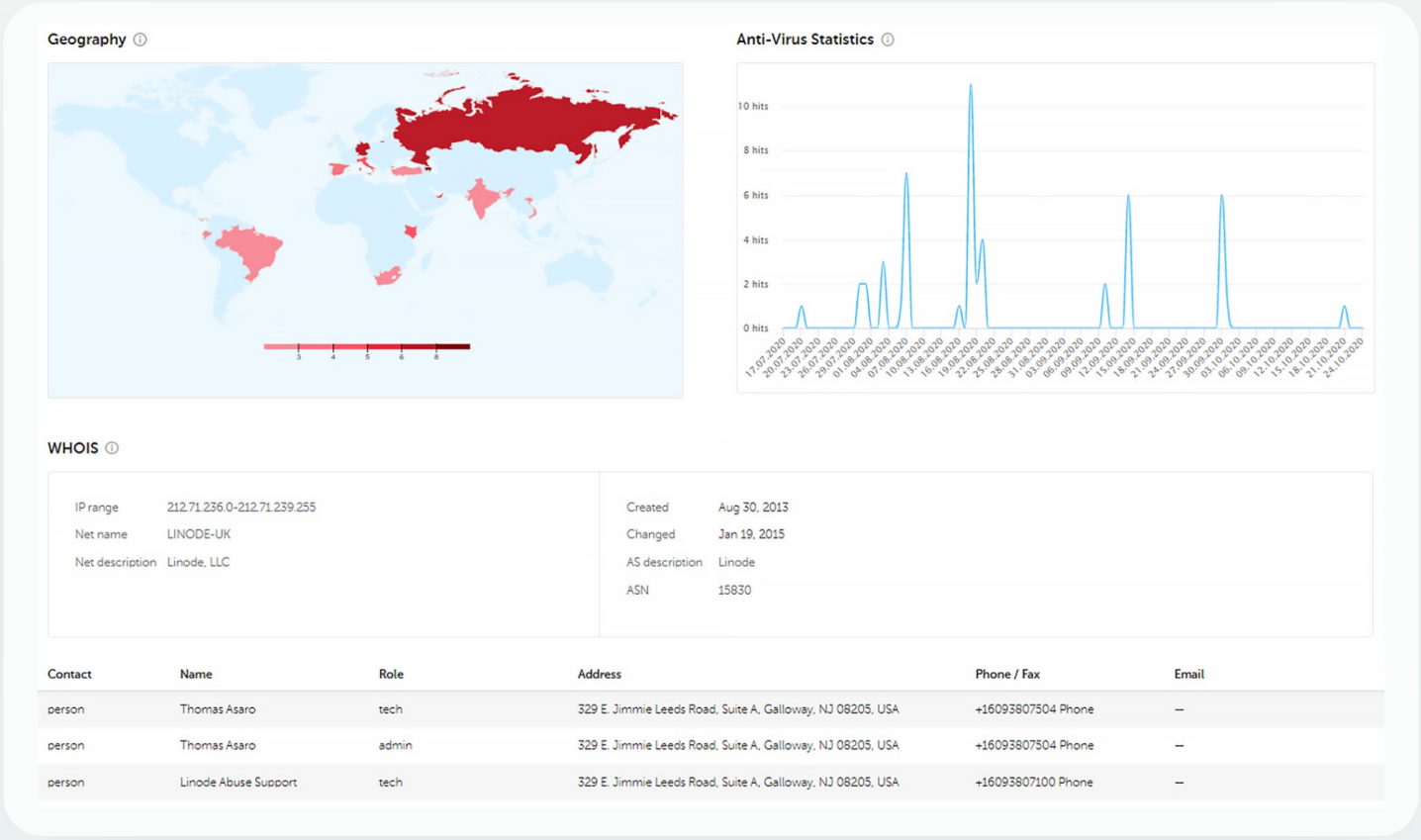
Faça diagnósticos e análises de incidentes de segurança em hosts e na rede de maneira mais eficiente, além de priorizar sinais de sistemas internos contra ameaças desconhecidas

Aprimore sua resposta a incidentes e funcionalidades de busca de ameaças para desfazer kill chains antes que os sistemas e dados cruciais sejam comprometidos

Procurar indicadores de ameaças através de uma interface baseada na Web ou através da API RESTful

Examinar detalhes avançados, incluindo certificados, nomes normalmente utilizados, caminhos de arquivo ou URLs relacionadas para descobrir novos objetos suspeitos

Verifique se o objeto descoberto pode ser considerado uma ameaça já disseminada ou única, e entenda por que um objeto deve ser tratado como malicioso

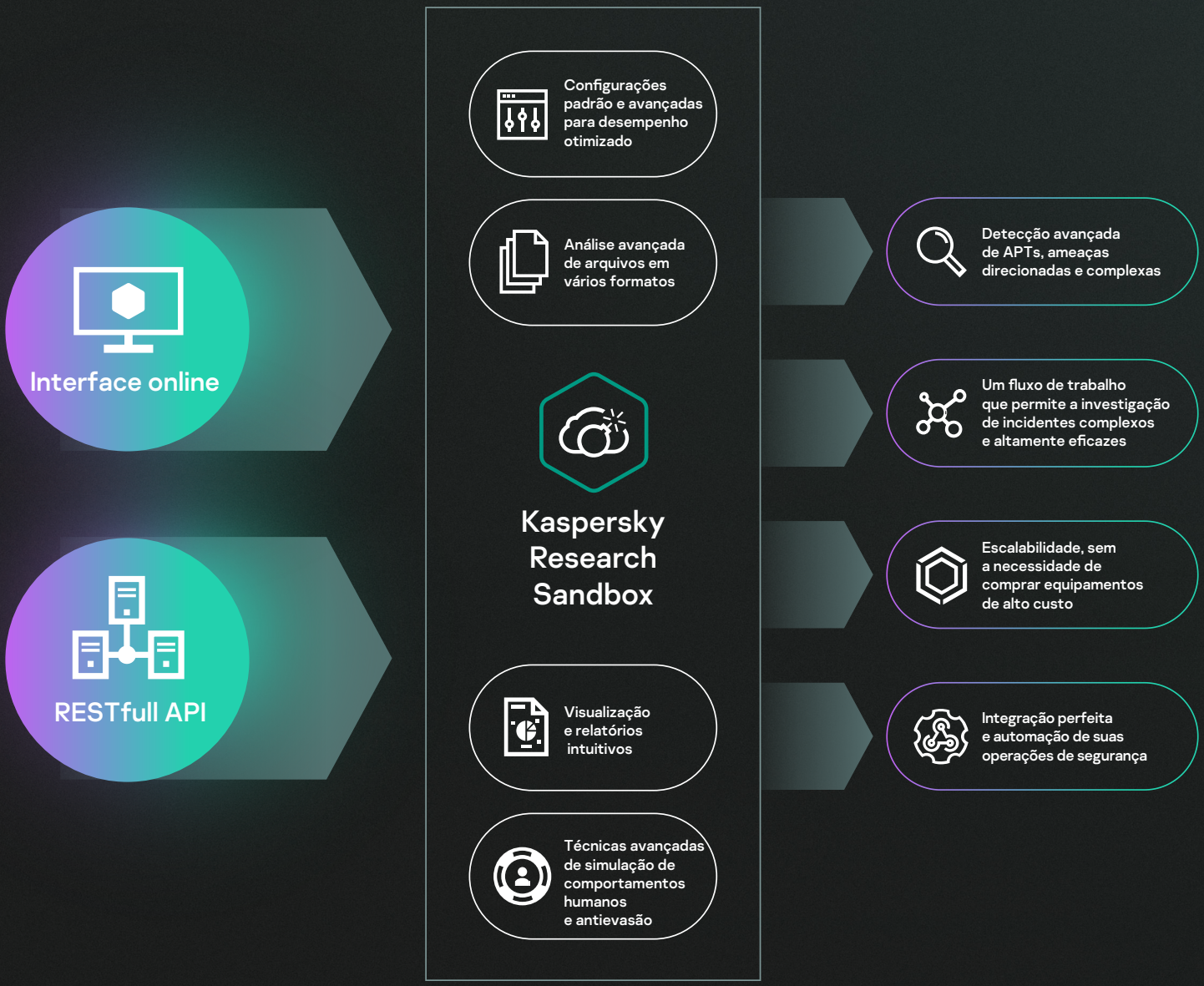


Kaspersky Research Sandbox

É impossível prevenir os ataques direcionados apenas com ferramentas AV tradicionais. Os mecanismos antivírus só são capazes de impedir ameaças conhecidas e suas variações, enquanto agentes de ameaças sofisticados usam um arsenal enorme de técnicas para burlar a detecção automática. Os prejuízos causados por incidentes de segurança da informação continuam a crescer, ressaltando a importância de recursos de detecção imediata de ameaças para garantir uma resposta rápida e a capacidade de combater ameaças antes que elas causem danos.

Tomar uma decisão inteligente com base no comportamento de um arquivo, analisando simultaneamente a memória de processo, a atividade de rede, etc. é a abordagem ideal para entender as ameaças direcionadas e personalizadas mais recentes e sofisticadas. Os dados estatísticos podem ter falta de informação sobre malware modificado, mas as tecnologias de sandbox são ferramentas poderosas que permitem a investigação das origens da amostra de arquivo, a coleta de IOC com base em análise comportamental e a detecção de objetos maliciosos nunca vistos.

O Kaspersky Research Sandbox permite investigar as origens de amostras de arquivos, coletar IOCs com base em análise comportamental e detectar objetos maliciosos que passaram despercebidos anteriormente. A solução oferece uma abordagem híbrida, que combina a inteligência de ameaças coletada de petabytes de dados estatísticos (graças ao Kaspersky Security Network e outros sistemas proprietários), análise comportamental e técnicas anti-evasão sólidas, com tecnologias que simulam ataques conduzidos por humanos, como clicker automático, navegação por documentos e processos do tipo 'dummy'.



Detecção e combate proativo de ameaças

O malware usa diversos métodos para impedir que sua execução seja detectada. Se o sistema não atender aos parâmetros necessários, o programa malicioso irá muito provavelmente autodestruir-se, sem deixar vestígios. Para o código malicioso ser executado, o ambiente de sandbox tem que conseguir imitar com precisão o comportamento normal de um usuário final.

O Kaspersky Cloud Sandbox oferece uma abordagem híbrida, que combina a inteligência de ameaças coletada a partir de petabytes de dados estatísticos (graças ao Kaspersky Security Network e outros sistemas proprietários), análise comportamental e técnicas anti-evasão sólidas, com tecnologias que simulam ações conduzidas por humanos, como clicker automático, document scrolling e processos do tipo 'dummy'.

Este serviço foi desenvolvido em nosso laboratório de sandbox interno, evoluindo por mais de uma década. A tecnologia incorpora todo nosso conhecimento sobre o comportamento de malware adquirido ao longo de 20 anos de pesquisa contínua de ameaças. Isso nos permite detectar mais de 400000 novos objetos maliciosos todos os dias para fornecer aos nossos clientes soluções de segurança líderes do setor.

O Kaspersky Research Sandbox pode ser gerenciado via a plataforma de gerenciamento central na nuvem, e um console offline em ambientes dispersos, aproveitando a inteligência contra ameaças e incorporando análises personalizáveis.

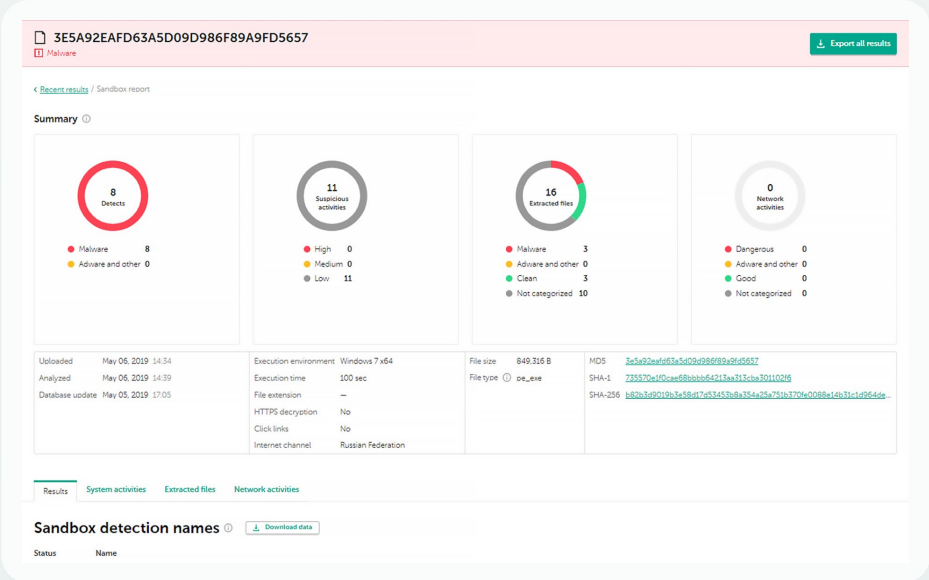
Como parte do Threat Intelligence Portal, o Kaspersky Research Sandbox é o componente final do nosso fluxo de trabalho de inteligência de ameaças. Enquanto a pesquisa de ameaças obtém a mais recente inteligência de ameaças detalhada sobre URLs, domínios, endereços de IP, hashes de arquivos, nomes de ameaças, dados estatísticos/comportamentais, dados de WHOIS/DNS etc., o Kaspersky Research Sandbox vincula esse conhecimento com os IOCs gerados pelo arquivo analisado.

Geração de relatórios abrangentes

- Pontuação unificada de ameaças
- Atividades suspeitas no sistema; com descrições detalhadas
- DLL carregados e executados
- Arquivos criados, modificados e eliminados
- Dumps de memória de processo e dumps de tráfego de rede (PCAP)
- Extensões mútuas criadas (mutexes)
- Chaves de registro modificadas e criadas
- Processos criados pelo arquivo executado
- Atividades de rede (sessões SMB, SMTP, IP, TCP, UDP, DNS, SSL, FTP, IRC, POP3, SOCKS; HTTP(s), solicitações e respostas)
- Inteligência de ameaças detalhada com contexto acionável para cada indicador de comprometimento (IOC) revelado
- Mapa detalhado de execução com técnicas MITRE ATT&CK em destaque
- O YARA detecta e aciona regras de IDS (incluindo regras personalizadas)
- Download e análise de arquivos hospedados em URLs
- Links clicáveis em documentos para Microsoft Office (Word, Excel, PowerPoint, Publisher, Outlook) e Adobe Reader
- Possibilidade de exportação dos detalhes da análise nos formatos STIX, JSON, CSV
- Variedade de ambientes, incluindo sistema operacional móvel (Android) e recursos de personalização de ambientes
- Parâmetros de execução de arquivo personalizados
- Diversos canais de Internet, possibilidade de rotear o tráfego através de canal VPN personalizado
- API RESTful
- Telas de captura e muito mais

Com o Kaspersky Research Sandbox, você pode executar investigações de incidentes altamente eficazes e complexas, obtendo um entendimento imediato da natureza da ameaça, depois fazer associações à medida que pesquisa mais fundo para revelar os indicadores de ameaça inter-relacionados.

A inspeção pode exigir muitos recursos, especialmente no que se refere a ataques com várias etapas. O Kaspersky Research Sandbox aumenta sua resposta a incidentes e atividades forenses, fornecendo a você a escalabilidade para processar arquivos automaticamente sem ter que comprar aparelhos caros ou se preocupar com recursos do sistema.



Kaspersky Threat Attribution Engine

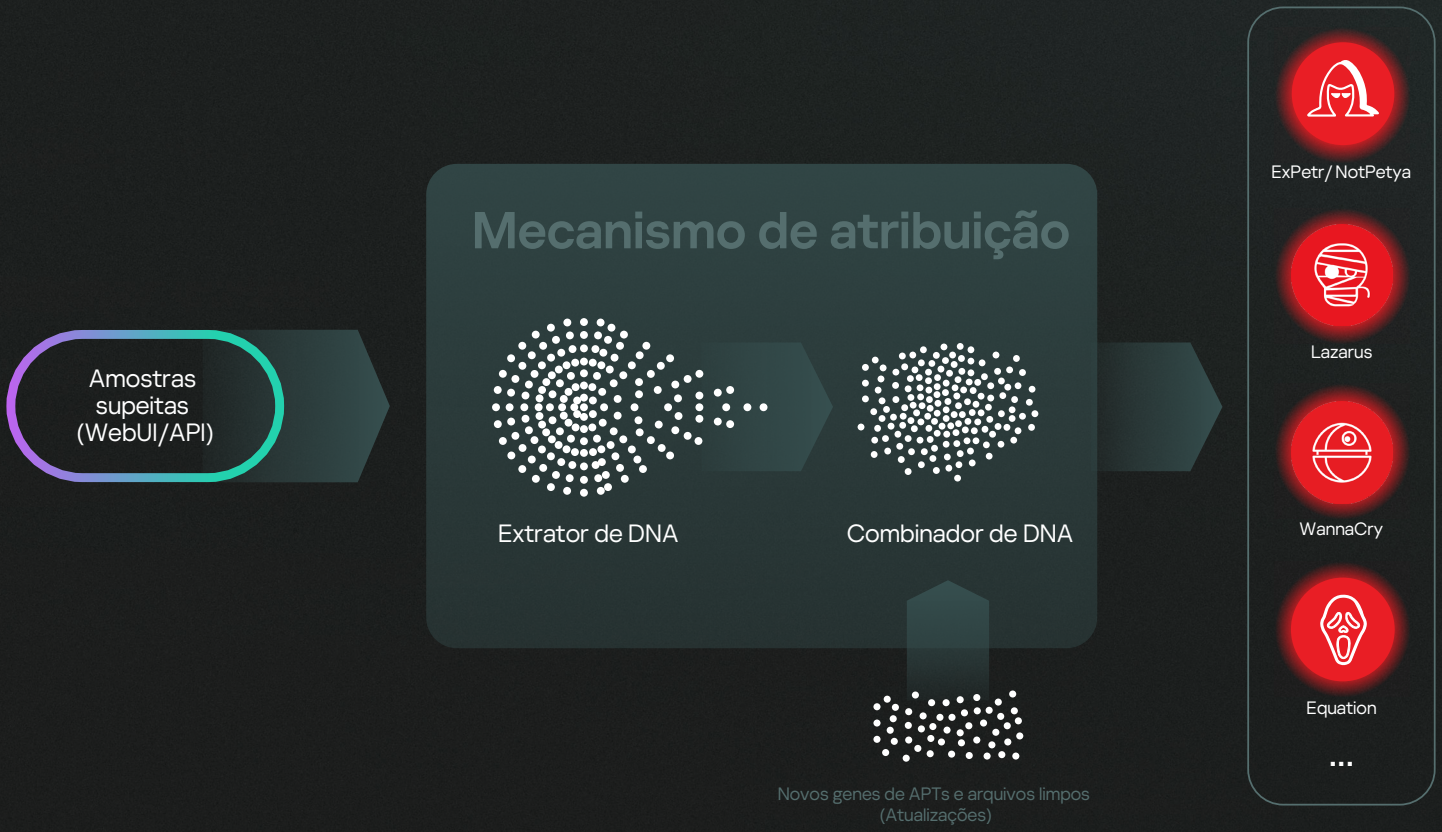
Há uma boa razão pela qual a atribuição de ameaças desempenha um papel tão importante na cibersegurança. O intervalo de tempo médio entre a detecção e a resposta a ameaças altamente sofisticadas pode ser prolongado e frustrante, devido à investigação complexa e aos processos de engenharia reversa envolvidos. Em muitos casos, esse intervalo pode dar aos invasores tempo suficiente para atingir seus objetivos.
A atribuição correta e no tempo oportuno ajuda não só a reduzir os tempos de resposta a incidentes de horas para minutos, mas também a reduzir o número de falsos positivos.

Identificar um ataque direcionado, traçar o perfil de invasores e criar fatores de atribuição para diferentes agentes de ameaça é um trabalho longo e complexo que pode levar anos. Criar uma atribuição de trabalho também requer uma grande quantidade de dados acumulados ao longo do tempo, bem como uma equipe de pesquisadores altamente qualificados com experiência de investigação relevante. Os pesquisadores geralmente acompanham a atividade de diferentes grupos e preenchem um banco de dados com todas as informações acumuladas. O banco de dados se torna então um recurso valioso que pode ser compartilhado como uma ferramenta.

O Kaspersky Threat Attribution Engine incorpora o banco de dados abrangente de amostras de malware de APT e de arquivos limpos coletados por especialistas da Kaspersky há mais de 25 anos. Rastreamos mais de 1.100 agentes e campanhas de ameaças e lançamos mais de 120 relatórios de inteligência de ameaças por ano. Nossas pesquisas contínuas servem como base para coleção de APT, que contém cerca de 83 mil arquivos. Isso melhora a detecção de sinalizações falsas e, em conjunto com ferramentas automatizadas, aumenta a precisão dos níveis de atribuição.

O produto oferece uma abordagem exclusiva para comparar amostras semelhantes, garantindo taxas de falsos positivos quase nulas. Qualquer ataque novo pode ser rapidamente vinculado a um malware de 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.

Como funciona?



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

1

Analisar a genética de uma amostra extraindo os seguintes elementos de seu código:

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

2

Pesquisa automática nos arquivos analisados de genótipos e strings semelhantes a genótipos e strings de amostras APT previamente analisadas ou já vinculadas a entidades de atribuição.

3

Com base em genótipos e sequências 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.

O produto pode ser implementado em um ambiente seguro de modo a restringir o acesso de terceiros às informações processadas e objetos enviados. Uma interface de API conecta o Engine a outras ferramentas e frameworks, de modo a implementar a atribuição em infraestruturas existentes e processos automatizados.

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)
- Permite a priorização eficiente de ameaças manuais ou automatizadas e triagem de alertas.
- Suporta a inclusão de amostras e agentes privados, instruindo o produto para detectar amostras que sejam semelhantes aos arquivos em suas coleções particulares.
- Permite uploads manuais de amostras e oferece a funcionalidade aprimorada da API REST para integração com fluxos de trabalho automatizados
- Oferece compatibilidade com a implementação no Amazon Web Services (AWS), permitindo configuração rápida do produto e economia de custos, sem nenhum investimento antecipado em hardware
- Exportação para regras YARA para pesquisa/verificação automatizada adicional de arquivos semelhantes ou integração com soluções de terceiros
- Facilidade de 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
- Permite descompactar arquivos protegidos por senha com senhas personalizadas
- Fornece acesso rápido à documentação e Contrato de Licença do Usuário Final (EULA) na interface web
- Envia atributos em arquivos paralelos para análise em uma única solicitação

Benefícios do Kaspersky Threat Attribution Engine

O Kaspersky Threat Attribution Engine calcula a pontuação de reputação

da amostra e revela sua genética e atribuição de código.; Isso fornece informações sobre a origem da amostra e pode permitir sua atribuição a possíveis autores.

Sua equipe de segurança pode adicionar suas próprias entidades privadas de atribução

e amostras relacionadas ao banco de dados do Kaspersky Threat Attribution Engine. A equipe pode, então, educar o aplicativo para atribuir amostras enviadas a essas amostras e entidades de atribuição privadas.

O processo de atribuição leva apenas alguns segundos

Com o Kaspersky Threat Attribution Engine, o processo de atribuição leva apenas alguns segundos, em comparação com os meses e anos necessários anteriormente.

O Kaspersky Threat Attribution Engine amplia e reforça

o portfólio Kaspersky para as Centrais de Operações de Segurança (SOCs) comerciais e agências nacionais de cibersegurança, apoiando-os no estabelecimento de um processo eficaz de gerenciamento de incidentes.

Kaspersky APT Intelligence Reporting

Os clientes do Kaspersky APT Intelligence Reporting recebem acesso contínuo exclusivo às nossas investigações e descobertas, incluindo dados técnicos completos (em vários formatos) sobre cada APT à medida que são descobertos, bem como sobre ameaças que nunca serão divulgadas. Os relatórios contêm um resumo executivo com informações fáceis de compreender orientadas ao C-Level, que descrevem o APT relacionado, juntamente com uma descrição técnica detalhada do APT com IOCs relacionados e regras YARA para fornecer aos pesquisadores de segurança, analistas de malware, engenheiros de segurança, analistas de segurança de rede e pesquisadores APT dados acionáveis que permitem uma resposta rápida e precisa à ameaça.

Nossos especialistas também alertam imediatamente sobre qualquer mudança que detectarem nas táticas de grupos de criminosos virtuais. Você também terá acesso ao banco de dados completo de relatórios APT da Kaspersky, outro poderoso componente de pesquisa e análise em suas defesas de segurança.

300+
agentes de ameaças

160+
relatórios privados por ano

+12,000
IoCs

400+
virtual

700+
Regras Yara

O Kaspersky APT Intelligence Reporting fornece

Perfis de agentes de ameaça

Mapeamento para MITRE ATT&CK

Sumário executivo

Informações orientadas para C-level

Análise técnica profunda
- Métodos de ataque
- Exploits usados
- Descrição de malware
- Infraestrutura C&C e descrição de protocolos
- Análise da vítima
- Análise de exfiltração de dados
- Atribuições

Conclusões e recomendações

Indicadores de Comprometimento (IOCs) e regras YARA

Benefícios do Kaspersky APT Intelligence Reporting

Informações sobre APTs não públicos

Por inúmeras razões, nem todas as ameaças de alto nível são divulgadas ao público geral — mas vamos compartilhá-las com você

Acesso privilegiado

Receba descrições técnicas sobre as ameaças mais recentes durante as investigações em andamento, antes de serem divulgadas ao público em geral

Análise retroativa

É fornecido acesso a todos os relatórios privados disponíveis durante todo o período da assinatura.

Acesso a dados técnicos

Inclui uma lista ampla de IOCs disponíveis nos formatos padrão, que incluem o openIOC ou o STIX, bem como acesso às nossas regras YARA

Dados de inteligência sobre perfis de agentes de ameaças

Incluindo o país de origem suspeito e a atividade principal, famílias de malware usadas, setores e regiões visadas e descrições de todos os TTPs usados, com mapeamento para MITRE ATT&CK

Integração e automação facilitadas

Integração e automação perfeitas dos seus fluxos de trabalho de segurança com RESTful API

Monitoramento contínuo de campanhas de APT.

Obtenha acesso a inteligência acionável durante investigações com informações sobre distribuição de APTs, IOCs, infraestruturas de comando e controle etc.

MITRE ATT&CK

Todos os TTPs descritos nos relatórios são mapeados para o MITRE ATT&CK, permitindo uma melhor detecção e resposta através do desenvolvimento e priorização dos casos de uso de monitoramento de segurança correspondentes, efetuando análises de falhas e testando as defesas atuais contra aos TTPs relevantes.

Kaspersky Crimeware Intelligence Reporting

O cibercrime com motivações financeiras não está limitado a setores específicos. E, embora ataques a infraestruturas financeiras como dispositivos de caixas eletrônicos e pontos de vendas continuem a ocorrer, todas as empresas em todos os setores estão em risco de sofrer ataques de ransomware. Nos últimos anos, houve uma diluição das fronteiras entre diferentes tipos de ameaças e diferentes tipos de agentes de ameaças. Isso inclui o surgimento de campanhas de ameaça persistente avançada (APT) focadas não em ciberespionagem, mas em furtos – roubo de dinheiro para financiar outras atividades em que o grupo de APT está envolvido. A crescente sofisticação das ameaças de softwares maliciosos não deve ser subestimada.

O Kaspersky Crimeware Intelligence Reporting permite que as organizações preparem suas estratégias defensivas ao fornecer informações atualizadas e imediatas sobre campanhas de malware, ataques direcionados a instituições financeiras e informações sobre ferramentas de crimeware usadas no ataque de bancos, empresas de processamento de pagamentos e suas infraestruturas específicas.

O Kaspersky Crimeware Intelligence Reporting fornece

- Descrições detalhadas de malware popular, amplamente disseminado e altamente conhecido
- Observações de pesquisadores/avisos antecipados, incluindo informações sobre ameaças de malware novas e atualizadas
- Informações sobre campanhas de malware perigosas e difundidas
- Descrição detalhada das ameaças voltadas para infraestruturas financeiras e as ferramentas de ataque correspondentes sendo desenvolvidas ou vendidas por cibercriminosos na Dark Web em várias regiões geográficas

Benefícios do Kaspersky Crimeware Intelligence Reporting

Acesso privilegiado

Receba descrições técnicas sobre as ameaças mais recentes durante as investigações em andamento, antes de serem divulgadas ao público em geral

Análise retroativa

É fornecido acesso a todos os relatórios privados disponíveis durante todo o período da assinatura.

Integração e automação facilitadas

Integração e automação perfeitas dos seus fluxos de trabalho de segurança com RESTful API

Acesso a dados técnicos

, incluindo uma lista ampla de IOCs disponíveis nos formatos padrão, que incluem o openIOC ou o STIX, bem como acesso às nossas regras YARA

Dados de inteligência sobre perfis de agentes de crimeware

Incluindo o país de origem suspeito e a atividade principal, famílias de malware usadas, setores e regiões visadas e descrições de todos os TTPs usados, com mapeamento para MITRE ATT&CK

Relatórios do Kaspersky ICS Threat Intelligence

O Kaspersky ICS Threat Intelligence Reporting fornece inteligência aprofundada e uma maior conscientização sobre campanhas maliciosas que visam organizações industriais, bem como informações sobre vulnerabilidades encontradas nos mais populares sistemas de controle industrial e tecnologias subjacentes. Os relatórios são entregues através do Kaspersky Threat Intelligence Portal, o que significa que você pode começar a utilizar o serviço imediatamente.

Todas as pesquisas de inteligência de ameaças relacionadas ao ICS são conduzidas por uma equipe dedicada, Kaspersky ICS CERT

- Estabelecida em 2016
- A primeira equipe CERT criada por uma organização comercial
- Cerca de 20 especialistas altamente qualificados em pesquisa de vulnerabilidade e ameaças ICS, resposta a incidentes e análise de segurança

Relatórios incluídos na sua assinatura

Relatórios de APTs

Relatórios sobre novas APT e campanhas de ataque de alto volume visando organizações industriais e atualizações sobre ameaças ativas

Vulnerabilidades detectadas

Relatórios sobre vulnerabilidades identificadas pela Kaspersky nos mais populares produtos utilizados nos sistemas de controle industrial, a internet das coisas industrial e infraestruturas em várias indústrias.

Análise e combate de vulnerabilidade.

Os nossos consultores fornecem recomendações acionáveis de especialistas da Kaspersky para ajudar a identificar e mitigar vulnerabilidades na sua infraestrutura.

A evolução do cenário de ameaças

Relatórios sobre as mudanças significativas no cenário de ameaças para sistemas de controle industriais, fatores críticos recém-descobertos que afetam os níveis de segurança de ICS e a exposição dos ICS a ameaças, incluindo informação específica da região, do país e do setor.

Com a inteligências de ameaças, você pode

Detectar e bloquear

ameaças reportadas para proteger bens digitais e físicos críticos, incluindo componentes de software e hardware, e assegurar a segurança e a continuidades de processos tecnológicos

Avaliar suas vulnerabilidades

Uma avaliação de vulnerabilidade dos seus materiais e ambientes industriais com base em avaliações precisas do escopo e a gravidade da vulnerabilidade, para tomar decisões informadas sobre o gerenciamento de correções ou a implementar outras medidas preventivas recomendadas pela Kaspersky

Correlacionar

Qualquer atividade maliciosa e suspeita que você detectar em ambientes industriais com os resultados de pesquisa da Kaspersky para atribuir sua detecção à campanha maliciosa em questão, identificar ameaças e responder prontamente a incidentes

Tirar vantagem de informações valiosas

Sobre tecnologias, táticas e procedimentos de ataque, vulnerabilidades recém-descobertas e outras mudanças importantes no cenário de ameaças para:

- Identifique e avalie os riscos das ameaças comunicadas e de outras ameaças semelhantes
- Planeje e projete alterações na infraestrutura industrial para assegurar a segurança da produção e continuidade do processo tecnológico
- Realize atividades de conscientização de segurança com base na análise de casos reais para criar cenários de treinamento de pessoal e planejar exercícios de equipe vermelha X equipe azul
- Tome decisões estratégicas informadas para investir em cibersegurança e para assegurar a resiliência das operações

Kaspersky Digital Footprint Intelligence

À medida que a sua empresa expande, a complexidade e a distribuição dos seus ambientes de TI também cresce, criando um desafio: proteger sua presença digital distribuída sem controle direto ou propriedade. Ambientes dinâmicos e interconectados permitem que as empresas obtenham benefícios significativos. No entanto, a interconetividade em constante crescimento está também expandindo a superfície de ataque. À medida que os invasores adquirem mais competências, é vital ter uma visão exata da presença online da sua organização, mas também monitorar suas mudanças e reagir a informações atualizadas sobre materiais digitais expostos.

As organizações usam uma ampla gama de ferramentas de segurança em suas operações de segurança, mas ainda existem ameaças digitais que exigem recursos muito específicos - para detectar e mitigar vazamentos de dados, monitorar planos e esquemas de ataque de cibercriminosos localizados em fóruns da dark web, etc. Para ajudar os analistas de segurança a explorar a visão do adversário sobre os recursos da sua empresa, ou descobrir a tempo os potenciais vetores de ataque em sua organização e ajustar as defesas de acordo, a Kaspersky criou o Kaspersky Digital Footprint Intelligence.

O Kaspersky Digital Footprint Intelligence fornece

Reconhecimento de rede

Identificação dos recursos de rede do cliente e serviços expostos que são um potencial ponto de entrada para um ataque. Análise personalizada das vulnerabilidades existentes, com pontuação e avaliação de risco abrangente adicionais baseadas na pontuação base do CVSS, disponibilidade de exploits públicos, experiência de testes de penetração e localização do recurso da rede (hospedagem/infraestrutura).

Proteção de marca

Monitoramento e bloqueio do uso não autorizado da marca online de uma empresa. Identificação de contas e aplicativos falsos de rede social, sites de phishing e outras atividades fraudulentas que podem prejudicar a reputação de uma empresa e/ou ludibriar clientes. Remoção de contas falsas em redes sociais e aplicativos falsos em lojas de aplicativos móveis.

Monitoramento da Dark Web

Monitoramento contínuo de domínios e recursos da Dark Web (fóruns, blogs de ransomware, messengers, sites portais etc.) para detectar quaisquer referências e ameaças relacionadas à sua empresa, clientes e parceiros. Análise de ataques direcionados ativos ou ataques que estejam sendo planejados, campanhas de APT direcionadas à sua empresa, setor ou região de operações.

Detecção de vazamentos de dados

Detecção de dados comprometidos de colaboradores, credenciais de parceiros e clientes, cartões bancários, números de telefone e outras informações confidenciais que podem ser usadas para perpetrar um ataque ou podem representar riscos para a reputação da empresa.

Fontes de inteligência

É vital que você adquira uma compreensão abrangente do seu nível de segurança externa.
Para fornecer essas informações, os analistas de segurança Kaspersky coletam e agregam informações extraídas das seguintes fontes de inteligência:

Seus dados não estruturados

- Endereços de IP
- Domínios da empresa
- Nomes de marcas
- Palavras-chave

Inventário de perímetro de rede

Web comum, deep web e dark web

Base de Conhecimento da Kaspersky

Relatórios analíticos

Alertas de ameaças

10 solicitações de derrubada por ano

Pesquisa em tempo real nos recursos da Kaspersky, OSINT, internet e dark web

Como funciona?

Configuração	Coleta	Filtragem	Resposta
Descoberta de informações sobre bens e materiais digitais da empresa	Coleta automatizada de dados da internet, deep e dark webs e do banco de dados sobre inteligência contra ameaças da Kaspersky	Detecção, análise e priorização de ameaças gerenciadas por analistas	Fornecimento de informações completas

Valor comercial

O Kaspersky Digital Footprint Intelligence oferece benefícios poderosos e alto valor agregado para a sua organização:

Proteja sua marca

Detecte ameaças potenciais em tempo real e proteja a reputação da sua empresa, preservando a confiança dos clientes, reduzindo o risco de prejuízos financeiros e danos às operações comerciais.

Reduza os riscos cibernéticos

Equipe seus principais agentes (diretoria e gestão) com informações sobre onde concentrar os gastos com cibersegurança, expondo deficiências na configuração atual e os riscos que elas representam.

Reaja com agilidade

O contexto adicional para alertas de segurança aprimora a resposta a incidentes e reduz o tempo médio de resposta (MTTR)

Reduza sua superfície de ataque

Gerencie a presença digital da sua empresa e controle os recursos de rede externos para combater vetores de ataque e vulnerabilidades que podem ser usados em um ataque.

Entre na mente de seus adversários

Prevenção e antecipação - saiba o que os cibercriminosos estão planejando e o que estão falando sobre a sua empresa na dark web e para que você possa estar preparado em caso de um ataque.

Domine o desconhecido

Melhore sua capacidade de resistir a ciberataques e de identificar ameaças fora do perímetro das equipes de segurança interna.

Kaspersky Takedown Service

Os cibercriminosos criam domínios maliciosos e de phishing que são usados para atacar sua empresa e suas marcas. A incapacidade de eliminar rapidamente essas ameaças, após serem identificadas, pode levar à perda de receita, danos à marca, perda de confiança dos clientes, vazamentos de dados e muito mais. Mas gerenciar o derrubamento desses domínios é um processo complexo, que requer experiência e tempo.

O Kaspersky Takedown Service combate rapidamente as ameaças de domínios maliciosos e de phishing antes que qualquer dano possa ser causado à sua marca e aos seus negócios. O gerenciamento de ponta a ponta de todo o processo economiza tempo e recursos valiosos dos clientes. O serviço de Takedown é fornecido globalmente.

A Kaspersky bloqueia mais de 15 mil URLs de phishing/scam e impede mais de um milhão de tentativas de clicar nesses URLs todos os dias. Graças aos vários anos de experiência na análise de domínios maliciosos e de phishing, sabemos como coletar todas as evidências necessárias para provar que eles são maliciosos. Cuidaremos do seu gerenciamento de remoção e permitiremos uma ação rápida para minimizar seu risco digital para que sua equipe possa se concentrar em outras tarefas prioritárias.

A Kaspersky oferece aos seus clientes proteção eficaz dos seus serviços online e reputação, trabalhando com organizações internacionais, agências nacionais e regionais de polícia (por exemplo, INTERPOL, Europol, Unidade de Crimes Digitais da Microsoft, Unidade Nacional de Crimes de Alta Tecnologia (NHTCU) da Agência Policial dos Países Baixos e The City of London Police), bem como Computer Emergency Response Teams (CERTs) em todo o mundo.

Como funciona?

Você pode solicitar diretamente através da Conta Corporativa Kaspersky, no nosso portal de suporte ao cliente corporativo. Prepararemos toda a documentação necessária e enviaremos a solicitação de remoção à autoridade local/regional relevante (CERT, registrador, etc.) que tenha os direitos legais necessários para encerrar o domínio. Você receberá notificações em todas as etapas até que o domínio solicitado seja derrubado com sucesso.

Proteção fácil de gerenciar

O Kaspersky Takedown Service elimina rapidamente as ameaças representadas por domínios maliciosos e de phishing antes que qualquer dano possa ser causado à sua marca e aos seus negócios. O gerenciamento de ponta a ponta de todo o processo economiza tempo e recursos valiosos.

Visibilidade completa

Você receberá notificações a cada etapa do processo, desde o registro da sua solicitação até a derrubada bem-sucedida

Gerenciamento de ponta a ponta

Gerenciaremos todo o processo de remoção e minimizaremos seu envolvimento.

Cobertura global

Seja qual for o local em que um domínio malicioso ou de phishing está registrado, a Kaspersky solicitará sua remoção da organização regional com a autoridade legal relevante.

Integração com o Kaspersky Digital Footprint Intelligence

O Kaspersky Takedown Service pode ser adquirido separadamente, mas sua integração com o Kaspersky Digital Footprint Intelligence aproveita ao máximo a sinergia natural entre esses serviços. O Kaspersky Digital Footprint Intelligence fornece notificações em tempo real sobre domínios de phishing e malware, que podem ser imediatamente enviados ao Kaspersky Takedown Service para bloqueio instantâneo.

Kaspersky Ask the Analyst

Cibercriminosos estão constantemente desenvolvendo novas formas sofisticadas de atacar empresas. O cenário de ameaças instável e de rápido crescimento da atualidade demonstra o uso de técnicas de ciberataques cada vez mais ágeis. As organizações enfrentam incidentes complexos causados por ataques em formato non-malware, fileless, do tipo living-off-the-land, exploits de dia zero, além de combinações de todas essas variantes incorporadas em ameaças complexas, ataques semelhantes a APT e direcionados.

Em uma época dominada por ciberataques direcionados a empresas de todos os tamanhos, profissionais de cibersegurança são mais importantes do que nunca, mas encontrá-los e retê-los não é tarefa fácil. E mesmo com uma equipe de cibersegurança bem estabelecida, seus especialistas nem sempre estão prontos para lutar na guerra contra ameaças sofisticadas sozinhos— eles precisam ser capazes de recorrer à assistência especializada de terceiros. A experiência externa pode esclarecer os caminhos prováveis de ataques complexos e APTs, fornecendo conselhos acionáveis sobre as melhores maneiras de eliminá-los.

A pesquisa de ameaças constante permite que a Kaspersky descubra, se infiltre e monitore comunidades fechadas e fóruns clandestinos frequentados por cibercriminosos em todo o mundo. Nossos analistas aproveitam o acesso à esses fóruns ocultos para detectar e investigar proativamente as ameaças mais prejudiciais e populares, bem como ameaças projetadas para organizações específicas

O serviço Kaspersky Ask the Analyst amplia mais ainda nosso Portfólio de Inteligência de Ameaças, permitindo que você solicite orientação e informações sobre ameaças específicas que está enfrentando ou nas quais está interessado. O serviço adapta os poderosos recursos de inteligência e pesquisa de ameaças da Kaspersky às suas necessidades específicas, permitindo que você monte defesas resilientes contra ameaças direcionadas à sua organização.

Benefícios do Kaspersky Ask the Analyst (assinatura unificada mediante solicitação)

APT e Crimeware

Informações adicionais sobre relatórios publicados e pesquisas em andamento (além do serviço APT ou Crimeware Intelligence Reporting)

Descrições de ameaças, vulnerabilidades e IoCs relacionados

- Descrição geral de famílias específicas de malware
- Contexto adicional para ameaças (hashes relacionados, URLs, CNCs etc.)
- Informações sobre uma vulnerabilidade específica (nível de gravidade e os mecanismos de proteção correspondentes nos produtos Kaspersky)

Solicitações relacionadas a ICS

- Informações adicionais sobre relatórios publicados
- Informações sobre vulnerabilidade do ICS
- Estatísticas e tendências de ameaças do ICS para região/setor
- Informações de análises de malware do ICS sobre regulamentações ou padrões

Inteligência de Dark Web

- Pesquisa na Dark Web sobre artefatos específicos, endereços de IP, nomes de domínio, nomes de arquivos, e-mails, links ou imagens
- Pesquisa e análise de informações

Malware analysis

- Análise de amostras de malware
- Recomendações sobre novas ações de remediação

Como funciona?

O Kaspersky Ask the Analyst pode ser comprado separadamente ou adicionado a qualquer um de nossos serviços de inteligência contra ameaças. Você pode solicitar diretamente através da Conta Corporativa Kaspersky, no nosso portal de suporte ao cliente corporativo. Responderemos por e-mail, mas se caso necessário e você estiver de acordo, podemos agendar uma teleconferência e/ou sessão com compartilhamento de tela para esclarecimentos. Após aceitar a sua solicitação, você receberá informações sobre o tempo estimado de processamento.

Casos de uso

1. Esclareça todos os detalhes em relatórios de inteligência de ameaças publicados anteriormente
2. Obtenha inteligência adicional para IoCs já fornecidos
3. Obtenha detalhes sobre vulnerabilidades e recomendações sobre como proteger-se contra exploits
4. Receba detalhes adicionais sobre as atividades específicas da Dark Web nas quais você está interessado
5. Obtenha um relatório geral da família de malware, incluindo o comportamento do malware, seu impacto potencial e detalhes sobre qualquer atividade relacionada que a Kaspersky tenha observado
6. Priorize efetivamente alertas/incidentes com informações contextuais detalhadas, além de categorização para IoCs relacionados fornecidas por meio de relatórios sintéticos
7. Solicite assistência para identificar se a atividade incomum detectada está relacionada a um APT ou agente de Crimeware
8. Envie arquivos de malware para análises completas, ajudando você a compreender o comportamento e a funcionalidade das amostras fornecidas

Benefícios do Kaspersky Ask the Analyst

Amplie seu conhecimento

Tenha acesso sob demanda a especialistas do setor, sem a necessidade de procurar ou investir na contratação de profissionais que são muitas vezes difíceis de encontrar

Agilize a investigação

Classifique e priorize incidentes eficazmente com base em informações contextuais detalhadas e personalizadas

Reaja rapidamente

Responda a ameaças e vulnerabilidades rapidamente, graças às nossas orientações sobre como bloquear ataques causados por vetores já conhecidos

Amplie seu conhecimento e recursos

O Kaspersky Ask the Analyst, oferece acesso à equipe principal de pesquisadores da Kaspersky, em uma base individualizada. O serviço oferece uma comunicação abrangente entre os especialistas para expandir suas capacidades atuais com nosso conhecimento e recursos exclusivos.

Conclusão

Combater as ciberameaças atuais requer uma visão completa das táticas e ferramentas utilizadas pelos agentes das ameaças. Gerar essa inteligência e identificar as contramedidas mais eficazes requer dedicação constante e altos níveis de especialização. Com petabytes de dados complexos de ameaças para extrair, tecnologias avançadas de Machine Learning e um grupo exclusivo de especialistas mundiais, nós trabalhamos para oferecer suporte aos nossos clientes do mundo todo com a mais recente inteligência de ameaças, ajudando-os a manter sua imunidade até mesmo em caso de ciberataques nunca vistos anteriormente.

Principais benefícios

Permite a visibilidade global de ameaças, a detecção imediata de ameaças virtuais, a priorização de alertas de segurança e uma resposta eficaz a incidentes de segurança da informação

Os insights exclusivos sobre as táticas, técnicas e procedimentos usados por agentes de ameaças em diferentes setores e regiões, permitem proteção proativa contra ameaças direcionadas e complexas

Uma visão geral abrangente da sua postura de segurança com recomendações acionáveis sobre estratégias de mitigação permite que você concentre sua estratégia defensiva em áreas identificadas como principais alvos de ataques virtuais

Poupa seus analistas e ajuda a focar sua força de trabalho em ameaças reais

Recursos aprimorados e acelerados de resposta a incidentes e busca de ameaças ajudam a reduzir o "tempo de permanência" do ataque e minimizar significativamente possíveis danos

Kaspersky Threat Intelligence

Saiba mais

www.kaspersky.com.br

#kaspersky
#bringonthefuture