kaspersky BRING ON THE FUTURE

Kaspersky Threat Attribution Engine

A tarefa de rastrear, analisar, interpretar e reduzir as ameaças de segurança de TI em constante evolução é complexa. A inteligência de ameaças tem um verdadeiro valor, além da tendência atual emergente na indústria de segurança de informações. E a atribuição de ameaças é provavelmente o ponto de interesse e contenção mais importante no tema de inteligência de ameaças.

Destaques do produto:

- Fornece acesso imediato a um repositório de dados selecionados sobre centenas de agentes e amostras de APT.
- 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 aberta para integração com fluxos de trabalho automatizados.
- Podem ser implantados em ambientes seguros para proteger seus sistemas e dados, bem como para atender a quaisquer requisitos de conformidade.
- Mantém absoluta privacidade e confidencialidade de todos os envios, a fim de evitar exposição informações sigilosas.

E o motivo é bem claro. O tempo médio entre a detecção e a resposta a ameaças altamente sofisticadas geralmente é muito longo devido aos processos complexos de investigação e de engenharia reversa. Em muitos casos, é o suficiente para que invasores atinjam 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 reduz 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 complexo que pode levar anos. A atribuição do trabalho de criação também requer anos de dados acumulados, além de uma equipe especializada de pesquisadores com experiência em investigação. Em resumo, os pesquisadores seguem a atividade de diferentes grupos e preenchem o banco de dados com as informações coletadas. Esse banco de dados se torna um recurso valioso que pode ser compartilhado como uma ferramenta.

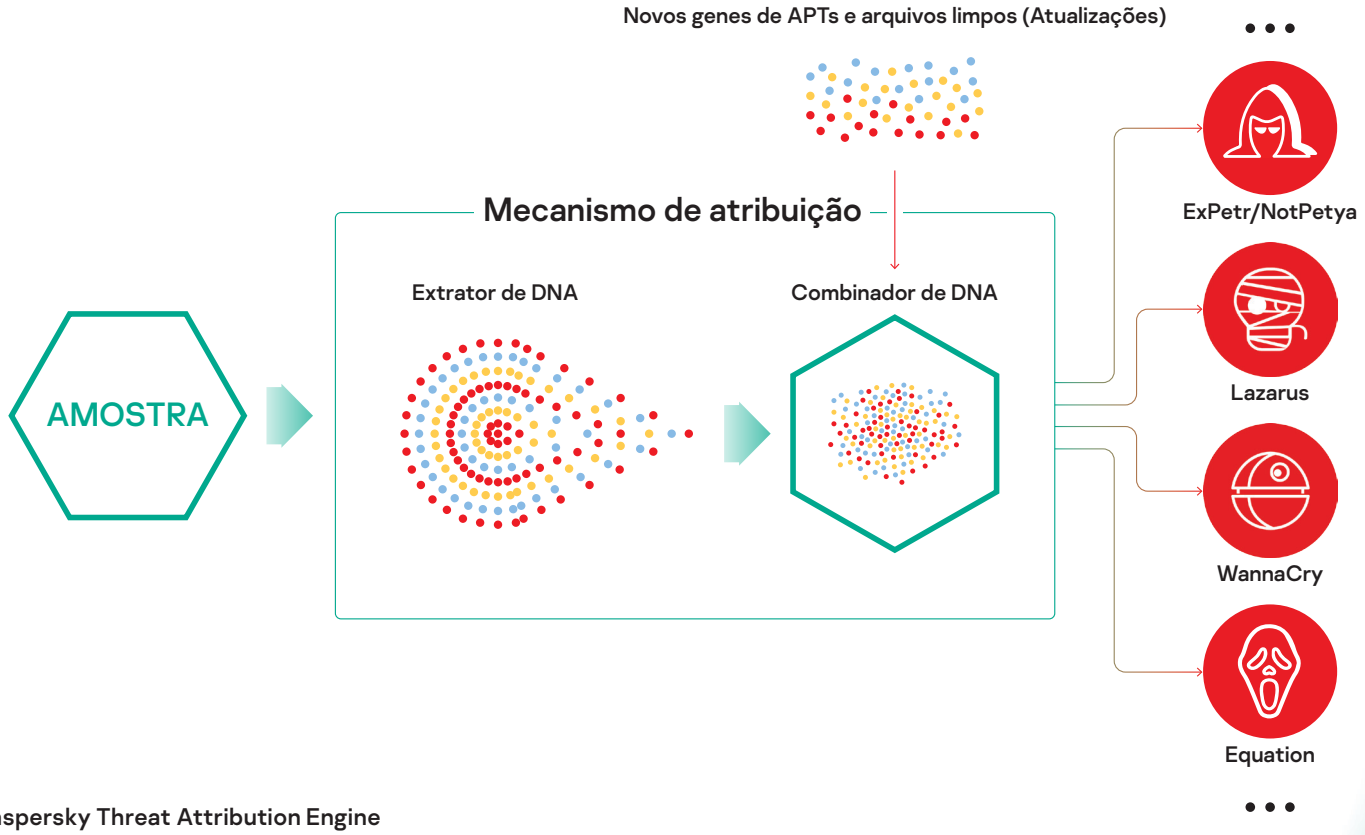
O Kaspersky Threat Attribution Engine incorpora o banco de dados de amostras de malware de APT e de arquivos limpos coletados por especialistas da Kaspersky ao longo dos últimos 22 anos. Rastreamos mais de 600 agentes de ameaças e campanhas com mais de 120 relatórios de inteligência de APT lançados todos os anos. Nossa pesquisa contínua serve como base para manter a precisão da grande coleção de APT, que contém mais de 60 mil arquivos. Ela melhora a detecção de sinalizações falsas e torna a atribuição a mais precisa possível usando ferramentas automáticas.

O produto permite uma abordagem exclusiva de comparação de amostras e garante taxas de zero falsos positivos. Com ela, é possível vincular rapidamente um novo ataque 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 sérios, além de permitir a tomada de medidas protetivas em tempo hábil para evitar que um invasor tenha acesso ao sistema.

Como funciona

O Kaspersky Threat Attribution Engine analisa a "genética" do malware, procurando similaridade entre códigos com amostras de APT anteriormenteinvestigadas e agentes vinculados, tudo isso de maneira automatizada. Ele compara os "genótipos", ou seja, peças binárias pequenas de arquivos decompostos, ao banco de dados de amostras de malware de APT e fornece um relatório da origem do malware, dos agentes de ameaça e da semelhança do arquivo com amostras de APT conhecidas.Além disso, o produto permite que as equipes de segurança adicionem agentes e objetos privados aos bancos de dados e instruem o produto a detectar amostras que sejam semelhantes aos arquivos na coleção particular. Com o Threat Attribution Engine, o processo de atribuição leva apenas alguns segundos, em comparação aos anos que eram necessários no passado.

O produto pode ser implantado em um ambiente seguro de modo a restringir o acesso de terceiros às informações processadas e objetos enviados. Ele conta com uma interface de API para conectar o Engine a outras ferramentas e frameworks, de modo a implementar a atribuição em infraestruturas existentes e processos automatizados.



Kaspersky Threat Attribution Engine

Informações detalhadas sobre o agente de APT relacionado podem ser encontradas nos relatórios Kaspersky APT Intelligence[1]. Como assinante do Kaspersky APT Intelligence Reporting, fornecemos a você acesso exclusivo e contínuo a nossas investigações e descobertas. Incluindo dados técnicos completos oferecidos em diversos formatos, em cada APT na forma em que se encontram, incluindo todas as ameaças que nunca serão publicadas.

O Kaspersky Threat Attribution Engine expande e fortalece ainda mais o portfólio da Kaspersky para agências de cibersegurança nacional e Centros de Operações de Segurança (SOCs) comerciais, apoiando-as no estabelecimento de processos de gerenciamento de incidentes eficientes.

O Kaspersky Attribution Engine melhora significativamente as operações de segurança, ajudando a:

- atribuir rapidamente arquivos a agentes APT conhecidos de modo a revelar motivações, métodos e ferramentas por trás dos incidentes;
- avaliar rapidamente se você é o alvo do ataque ou uma vítima colateral para configurar procedimentos de contenção e resposta adequados;
- garantia efetiva diminuição de ameaças e em tempo adequado de acordo com a inteligência de ameaça apropriada na família APT fornecida no Kaspersky APT Intelligence Reporting.

1 Uma assinatura do Kaspersky APT Intelligence Reporting deve ser adquirida separadamente

Notícias sobre ameaças virtuais: www.securelist.com
Notícias sobre segurança de TI: business.kaspersky.com
Segurança de TI para PMEs: kaspersky.com.br/business
Segurança de TI para empresas: kaspersky.com.br/enterprise

www.kaspersky.com.br

Somos comprovados. Somos independentes. Somos transparentes. Estamos empenhados em construir um mundo mais seguro, onde a tecnologia melhora as nossas vidas. É por isso que criamos soluções de segurança. Para que todas as pessoas, em todos os lugares, possam aproveitar as infinitas oportunidades que a tecnologia oferece. Antecipe sua cibersegurança para um futuro mais seguro.

Saiba mais em kaspersky.com.br/transparency

Proven.
Transparent.
Independent.