Kaspersky Research Sandbox

kaspersky BRING ON THE FUTURE

Tecnologias de sandbox

As tecnologias de sandbox são ferramentas poderosas que permitem investigar as origens de um objeto, coletar IOCs baseados em análises comportamentais e detectar objetos mal-intencionados inéditos.

Kaspersky Research Sandbox

Tomar uma decisão inteligente com base no comportamento de um arquivo ou URL, analisando simultaneamente a memória de processos, a atividade de rede etc., é a abordagem ideal para entender as ameaças sofisticadas, direcionadas e personalizadas atuais.

O malware de hoje usa diversos métodos para evitar a execução de seu código caso isso possa expor sua atividade mal-intencionada. Se o sistema não cumprir os parâmetros necessários, o programa malicioso irá muito provavelmente autodestruir-se, sem deixar vestígios. Para que o código mal-intencionado seja executado, o ambiente de sandbox deverá conseguir imitar com exatidão o comportamento normal de um usuário final.

O Kaspersky Research Sandbox foi desenvolvido diretamente em nosso complexo de sandbox em laboratório, uma tecnologia que está evoluindo há uma década. Ele incorpora todo o conhecimento sobre comportamentos de malware que adquirimos por meio de nossa constante pesquisa sobre ameaças, possibilitando que detectemos mais de 380.000 novos objetos mal-intencionados todos os dias. Implantada localmente, essa nova tecnologia avançada também evita a exposição de dados fora da organização.

Ela oferece uma abordagem híbrida, combinando análise comportamental e técnicas antievasão, com tecnologias de simulação humana. O Kaspersky Research Sandbox também permite personalização de imagens do sistema para análise, adequando-as a ambientes reais, o que aumenta a precisão da detecção de ameaças e a velocidade de investigação.

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
- A implantação local garante que nenhum dado seja exposto fora da organização
- Técnicas antievasão avançadas e tecnologias de simulação humana
- Envio de arquivo/URL manual e API RESTful
- Suporte à análise de mais de 100 tipos de arquivos com relatórios de análise detalhados
- Regras Suricata personalizadas para verificar tráfego de rede podem ser adicionadas e usadas junto com regras Suricata prontas
- O produto é compatível com implantações bare metal e pode ser facilmente dimensionado de acordo com o desempenho necessário

Arquitetura de alto nível do Kaspersky Research Sandbox

O produto é compatível com implantações bare metal. A configuração de hardware depende do desempenho necessário e pode ser dimensionada. Ela requer conexão de rede de 100 Mbps para cada canal e pelo menos uma conexão ISP independente (duas ou mais são recomendadas para tolerância a falhas). O ISP deve conhecer e estar pronto para tráfego mal-intencionado.

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, ele 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 dentro da máquina virtual para que o código mal-intencionado seja forçado a ser executado mais cedo.

O malware pode não mostrar seu comportamento mal-intencionado se ele estiver destinado a um aplicativo específico que esteja ausente na sandbox. Para resolver esse desafio, os pesquisadores devem revisar logs, compreender o que está faltando, adicioná-lo a uma máquina virtual e executar esse processo novamente. Quando o malware tentar acessar um aplicativo, o sistema patenteado interceptará essa tentativa. Ele não vai esperar até que a execução do arquivo seja concluída, em vez disso, pausará o processo para criar o aplicativo e o conteúdo necessários.

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

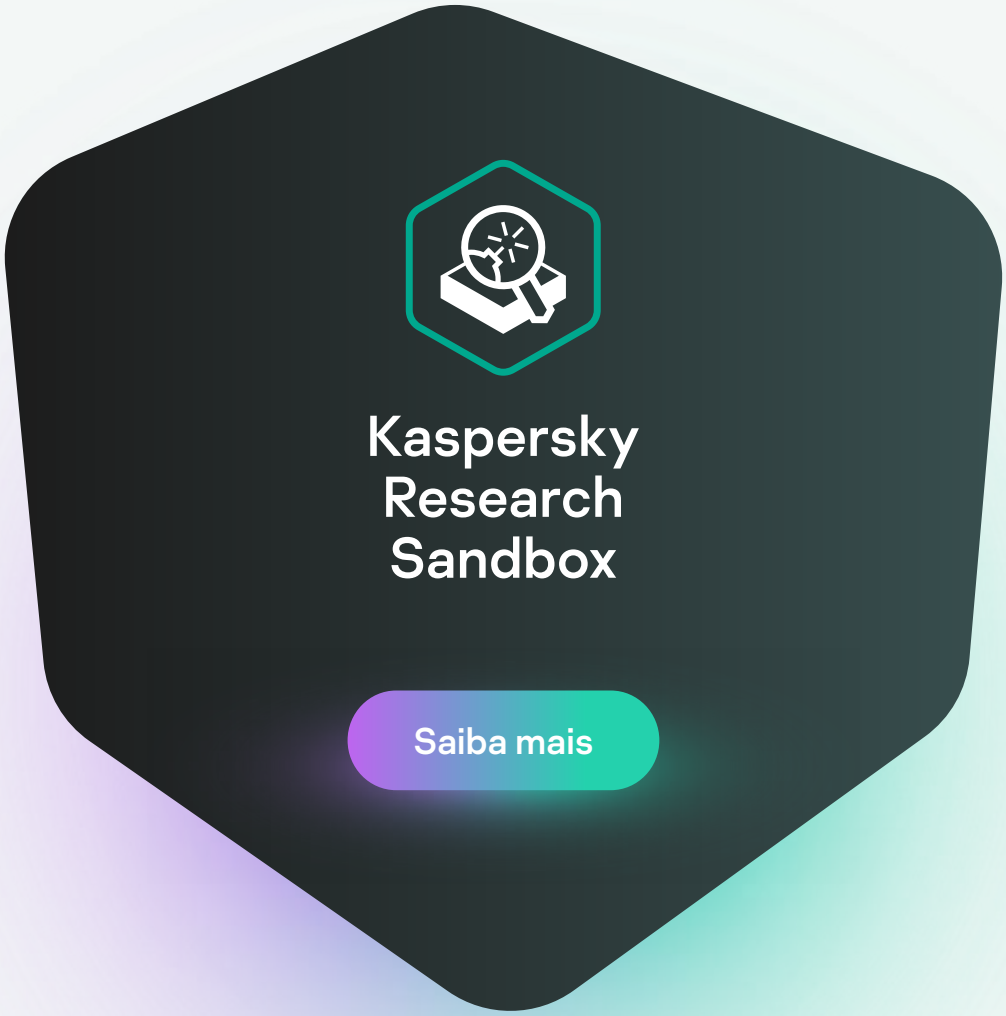
Despejo do tráfego de rede (PCAP)

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.

O Kaspersky Research Sandbox é o instrumento apropriado para detecção de ameaças desconhecidas. Ele é mais maduro e mais focado em ameaças avançadas do que qualquer outra solução.



www.kaspersky.com.br