kaspersky BRING ON THE FUTURE

Kaspersky Research Sandbox

Intelligente Entscheidungen auf Basis von Dateiverhalten zu treffen und zugleich etwa den Prozess-Arbeitsspeicher, die Netzwerkaktivität usw. zu analysieren, ist der optimale Ansatz, um ausgeklügelte, gezielte und maßgeschneiderte Bedrohungen von heute zu erfassen. Sandboxing-Technologien sind leistungsstarke Werkzeuge, die die Untersuchung der Herkunft von Beispieldateien, die Sammlung von IoCs auf der Grundlage einer Verhaltensanalyse und die Erkennung von Schadobjekten, die zuvor nicht erkannt wurden, ermöglichen.

Vorteile des Produkts im Überblick:

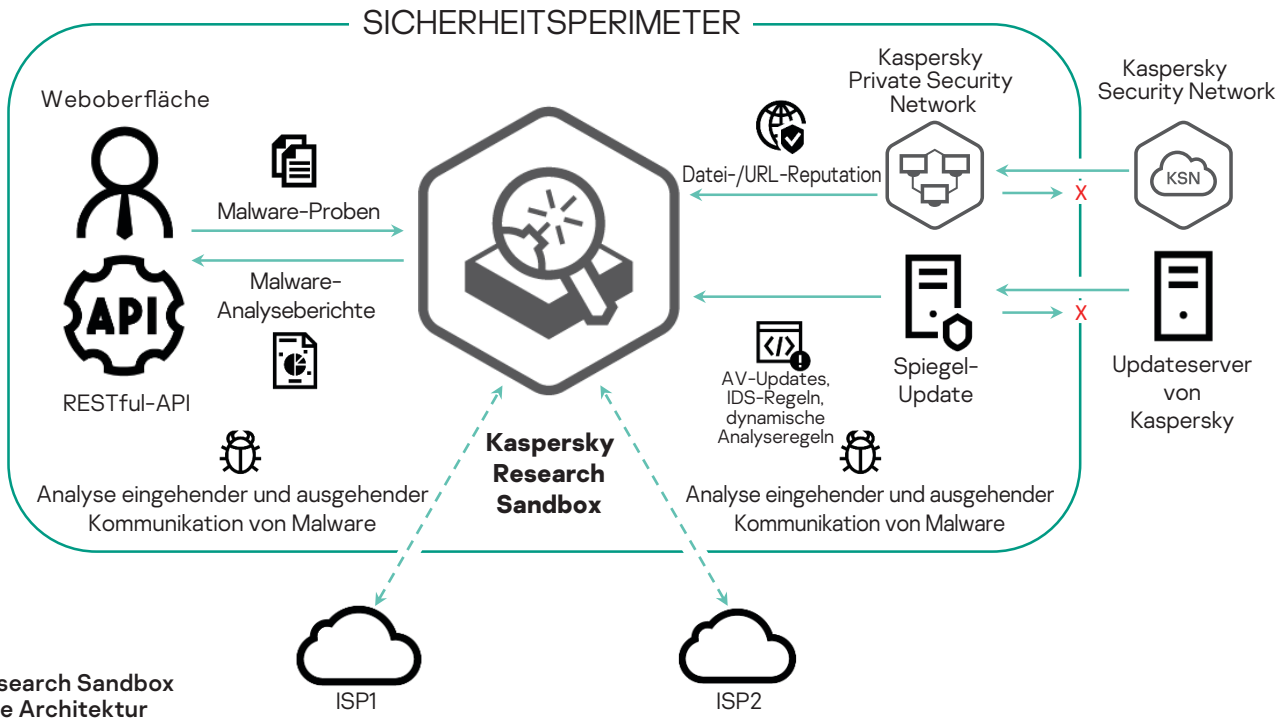
- Lokale Implementierung, damit keine Daten das Unternehmen verlassen müssen
- Unterstützt die Analyse von mehr als einhundert Dateitypen
- Fortschrittliche Anti-Umgehungstechniken
- Emulation von Benutzeraktivitäten
- Angepasste Images, um Bedrohungen über eine Reihe von Betriebssystemen und Softwareprogrammen zu analysieren, und nur auf Basis realer Umgebungen
- Separate Analyse jedes einzelnen Prozesses, um verdächtige Aktivitäten an zugehörigen Netzwerkverbindungen zu erkennen
- Detaillierte Analyseberichte mit sämtlichen Systemaktivitäten, extrahierten Dateien, Netzwerkaktivitäten (PCAP) und grafischen Übersichten
- Unterstützt die Integration mit Kaspersky Private Security Network
- Manuelle Dateiübermittlung und RESTful-API für nahtlose Integration und Automation Ihrer Sicherheitsworkflows

Heute kommt bei Malware eine Vielzahl von Methoden zum Einsatz, um die Ausführung des eigenen Codes zu vermeiden, wenn dies zur Aufdeckung der schädlichen Aktivität führen könnte. Wenn das System die erforderlichen Parameter nicht erfüllt, zerstört sich das schädliche Programm selbst, ohne Spuren zu hinterlassen. Damit der Schadcode ausgeführt werden kann, muss die Sandboxing-Umgebung daher in der Lage sein, ein normales Nutzerverhalten genau nachzuahmen.

Kaspersky Research Sandbox geht unmittelbar aus unserem hauseigenen Sandboxing-Komplex hervor, den wir seit über 10 Jahren stetig weiterentwickeln. Er umfasst das gesamte Wissen über Malware-Verhalten, das Kaspersky im Laufe seiner kontinuierlichen Bedrohungserforschung gesammelt hat und uns in die Lage versetzt, mehr als 350 000 neue schädliche Objekte pro Tag zu erkennen. In einer lokalen Bereitstellung verhindert diese leistungsstarke Technologie auch die Gefährdung von Daten außerhalb der Organisation.

In einem hybriden Ansatz werden Verhaltensanalysen und beinharte Anti-Umgehungstechniken mit Technologien zur Simulation menschlichen Verhaltens kombiniert. Mit der Kaspersky Research Sandbox werden außerdem angepasste Images der zu analysierenden Systeme erstellt und auf reale Umgebungen zugeschnitten, was die Genauigkeit der Bedrohungserkennung und das Ermittlungstempo erhöht.

In der Übersicht unten ist die übergeordnete Architektur der Kaspersky Research Sandbox dargestellt.



Kaspersky Research Sandbox übergeordnete Architektur

Um sich selbst zu schützen, kann eine schädliche Datei erst prüfen, ob es sich in einer virtuellen Maschine befindet, und sich eine Zeit lang inaktiv bleiben, bis die Sandbox sich anderem zuwendet. In solchen Fällen beschleunigt die patentierte Technologie den Lauf der Zeit innerhalb der virtuellen Maschine, so dass der Schadcode früher zur Ausführung gezwungen ist.

Malware legt ihr schädliches Verhalten eventuell nicht offen, wenn sie auf ein bestimmtes Programm ausgelegt ist, das in der Sandbox nicht vorhanden ist. Um diese Herausforderung zu meistern, müssen die Malware-Analysten Protokolle durchgehen, um in Erfahrung zu bringen, was fehlt. Dann können sie das Programm auf einer virtuellen Maschine installieren und den Prozess erneut starten. Wenn die Malware daraufhin versucht auf das Programm zuzugreifen, wird sie von dem patentierten System daran gehindert. Dabei wird das Ende der Dateiausführung nicht abgewartet, sondern der Prozess wird auf Pause gesetzt, bis das benötigte Programm und der Inhalt erstellt sind.

Erkennungsregeln, die beschreiben, wie auf ein bestimmtes Ereignis zu reagieren ist, werden nicht vorinstalliert oder innerhalb der Engine implementiert, sondern können ganz einfach aktualisiert und hinzugefügt werden.

Kaspersky Research Sandbox basiert auf einer patentierten firmeneigenen Technologie (Patent Nr. US10339301). Durch Nachstellen der exakten Bedingungen, unter denen die Malware zur Ausführung gebracht wird, genügt Forschern ein einziger Versuch, um eine verdächtige Datei analysieren zu können.

Das Produkt unterstützt eine Bare-Metal-Bereitstellung. Die Hardwarekonfiguration hängt von der benötigten Leistung ab und ist entsprechend skalierbar. Für jeden Kanal werden eine Netzwerkverbindung mit 100 Mbit/s und mindestens eine unabhängige ISP-Verbindung benötigt (aus Gründen der Fehlertoleranz werden zwei oder mehr empfohlen). Der ISP sollte auf schädlichen Datenverkehr eingerichtet und vorbereitet sein.

Nach Abschluss der Analyse stellt Research Sandbox einen detaillierten Bericht zu Verhalten und Funktion der analysierten Probe zusammen, auf dessen Grundlage Sie angemessene Abwehrverfahren definieren können:

- **Zusammenfassung**: Allgemeine Informationen zum Ergebnis der Ausführung einer Datei
- **Von Sandbox ermittelte Namen**: eine Liste der Erkennungen (sowohl AV als auch Verhalten), die während der Dateiausführung registriert wurden
- **Ausgelöste Netzwerkregeln**: eine Liste der SNORT-Regeln des Netzwerks, die bei der Datenverkehranalyse vom ausgeführten Objekt ausgelöst wurden
- **Ausführungsübersicht**: grafische chronologische Darstellung der Objektaktivitäten (an Dateien, Prozessen und der Registry ausgeführte Aktionen sowie Netzwerkaktivitäten) und deren gegenseitige Abhängigkeiten. Der Root-Node des Baums steht für das ausgeführte Objekt
- **Verdächtige Aktivitäten**: eine Liste der registrierten verdächtigen Aktivitäten
- **Screenshots**: ein Satz von Screenshots, die während der Dateiausführung aufgenommen wurden
- **Geladene PE-Images**: eine Liste der geladenen PE-Images, die während der Dateiausführung erfasst wurden
- **Dateioperationen**: eine Liste der während der Dateiausführung registrierten Dateioperationen
- **Registry-Zugriffe**: eine Liste der Operationen, die während der Dateiausführung an der Registry des Betriebssystems durchgeführt wurden
- **Prozessoperationen**: eine Liste der Interaktionen mit verschiedenen Prozessen, die während der Dateiausführung registriert wurden
- **Synchronisierungsvorgänge**: eine Liste der Operationen an erstellten Synchronisierungsobjekten (Mutex, Event, Semaphore), die während der Dateiausführung registriert wurden
- **Heruntergeladene Dateien**: eine Liste der Dateien, die während der Dateiausführung aus dem Netzwerkverkehr extrahiert wurden
- **Abgelegte Dateien**: eine Liste der Dateien, die von der ausgeführten Datei gespeichert (erstellt oder modifiziert) wurden
- **HTTPS/HTTP/DNS-Anforderungen**: Listen von HTTPS-/ HTTP-/ DNS-Anforderungen, die während der Dateiausführung registriert wurden
- **Netzwerkverkehr-Dump (PCAP)**: Netzwerkaktivitäten können im PCAP-Format exportiert werden

Kaspersky Research Sandbox ist die erste Wahl, wenn es um die Erkennung unbekannter Bedrohungen geht. Sie ist hoch entwickelt und besser auf hochentwickelte Bedrohungen spezialisiert als jede andere Lösung.

Cyber Threat News: https://de.securelist.com/
IT Security News: https://www.kaspersky.de/blog/b2b/
IT-Sicherheit für KMU: kaspersky.de/business
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise

www.kaspersky.de

Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir wollen eine sichere Umgebung schaffen, in der Technologie unser Leben verbessert. Deshalb schützen wir diese Technologien, damit Menschen auf der ganzen Welt die unzähligen technologischen Möglichkeiten nutzen können. Wir tragen mit Cybersicherheit zu einer sicheren Zukunft bei.

Erfahren Sie mehr unter kaspersky.de/transparency

Proven.
Transparent.
Independent.