Kaspersky Research Sandbox

kaspersky BRING ON THE FUTURE

Sandboxing-Technologien

Sandboxing-Technologien sind leistungsstarke Tools, die die Untersuchung der Herkunft von Beispieldateien, die Sammlung von IoCs auf der Grundlage einer Verhaltensanalyse und die Erkennung von zuvor unerkannten Schadobjekten ermöglichen.

Kaspersky Research Sandbox

Intelligente Entscheidungen auf Basis von Datei- oder URL-Verhalten zu treffen und zugleich etwa den Prozess-Arbeitsspeicher, die Netzwerkaktivität usw. zu analysieren, ist der optimale Ansatz, um selbst die komplexesten Bedrohungen zu erfassen.

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.

Die Kaspersky Research Sandbox geht unmittelbar aus unserem Sandboxing-Komplex hervor – eine Technologie, die wir seit über 10 Jahren stetig weiterentwickeln. Sie umfasst das gesamte Wissen über Malware-Verhalten, das wir im Laufe unserer kontinuierlichen Bedrohungsforschung gesammelt haben. So konnten wir mehr als 380.000 neue schädliche Objekte pro Tag erkennen. In einer lokalen Bereitstellung verhindert diese leistungsstarke Technologie auch die Gefährdung von Daten außerhalb der Organisation.

In einem hybriden Ansatz werden Verhaltensanalysen und Anti-Umgehungstechniken mit Technologien zur Simulation menschlichen Verhaltens kombiniert. Mit der Kaspersky Research Sandbox lassen sich außerdem angepasste Images der zu analysierenden Systeme erstellen und auf reale Umgebungen zuschneiden. Dies erhöht die Genauigkeit der Bedrohungserkennung und das Ermittlungstempo.

Vorteile des Produkts im Überblick:

- Automatisierte Objektanalyse in Windows, Linux und Android
- Dank der Anpassbarkeit der Images kann die Bedrohungsanalyse in verschiedensten Betriebssysten und Programmen (nur solche, die sich auf reale Umgebungen beziehen) unter Windows durchgeführt werden
- An der Bewertungszahl, die sich aus Metriken und Daten bei der Dateiausführung ergeben, lässt sich der Risikograd des analysierten Objekts ablesen
- Lokale Implementierung, damit keine Daten das Unternehmen verlassen müssen
- Erweiterte Anti-Umgehungs-Techniken und Technologien zur Simulation menschlichen Verhaltens
- Manuelles Einreichen von Dateien/URLs und RESTful API
- Für mehr als 100 Dateitypen können Analysen durchgeführt und detaillierte Berichte erstellt werden
- Suricata-Regeln zum Scannen des Netzwerkverkehrs können individuell angepasst und zusammen mit den standardmäßigen Suricata-Regeln genutzt werden
- Das Produkt unterstützt eine Bare-Metal-Bereitstellung und ist so je nach erforderlichem Leistungsumfang beliebig skalierbar

Kaspersky Research Sandbox: High-Level-Architektur

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.

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 Experten ein einziger Versuch, um eine verdächtige Datei/URL analysieren zu können.

Um sich selbst zu schützen, prüfen einige schädliche Dateien erst, ob sie sich in einer virtuellen Maschine befinden, und bleiben inaktiv, bis sich die Sandbox anderem zuwendet. In solchen Fällen beschleunigt die patentierte Technologie den Lauf der Zeit innerhalb der virtuellen Maschine, so dass der Schadcode vorzeitig 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 Malware-Analysten anhand von Protokollen ermitteln, 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.

Detaillierte Analyseberichte

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

Fazit

Allgemeine Informationen über die Ergebnisse einer Dateiausführung bzw. dem Öffnens einer URL

Ermittelte Namen

Eine Liste der Erkennungen (sowohl AV als auch Verhalten), die während der Dateiausführung registriert wurden

Ausgelöste Netzwerkregeln

Eine Liste der Suricata-Regeln des Netzwerks, die bei der Datenverkehranalyse vom ausgeführten Objekt ausgelöst wurden

Ausführungsübersicht

Chronologische grafische Darstellung der Objektaktivitäten und deren Wechselbeziehungen

Verdächtige Aktivitäten

Eine Liste der registrierten verdächtigen Aktivitäten

Screenshots

Screenshots, die während der Dateiausführung bzw. beim Öffnen einer URL aufgenommen wurden

Geladene PE-Images

Eine Liste der geladenen PE-Images, die während der Dateiausführung bzw. dem Öffnen einer URL erfasst wurden

Dateioperationen

Eine Liste der während der Dateiausführung bzw. beim Öffnen einer URL registrierten Dateioperationen

Registry-Zugriffe

Eine Liste der Operationen, die während der Dateiausführung bzw. beim Öffnen einer URL 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 bzw. beim Öffnen einer URL registriert wurden

Dateidownloads

Eine Liste der Dateien die während der Dateiausführung bzw. beim Öffnen einer URL aus dem Netzwerkverkehr extrahiert wurden

Abgelegte Dateien

Eine Liste der Dateien, die von der ausgeführten Datei gespeichert (erstellt oder modifiziert) wurden

HTTPS/HTTP/DNS/IP/TCP/UDP usw.

Details von Netwerksitzungen/-anforderungen, die während der Dateiausführung bzw. beim Öffnen einer URL registriert wurden

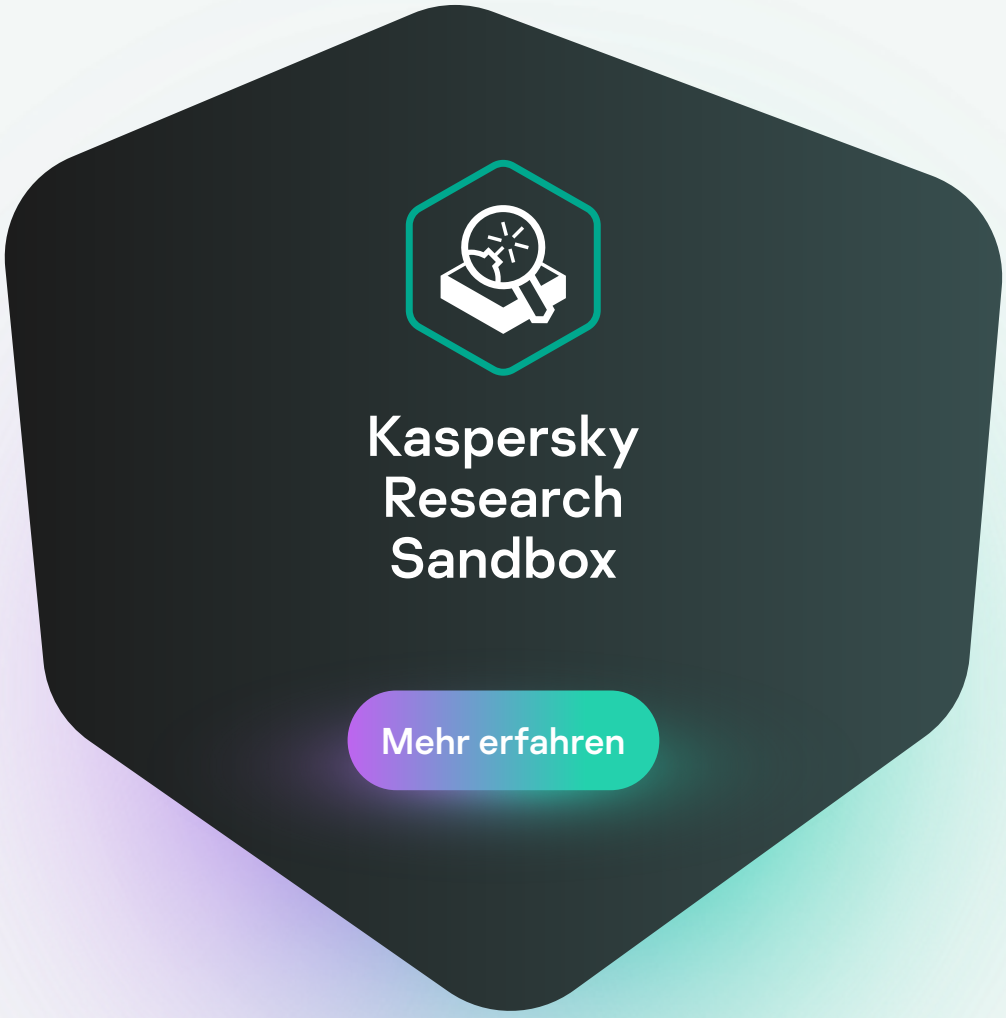
Netzwerkverkehrsauszüge (PCAP)

Netzwerkaktivitäten können im PCAP-Format exportiert werden.

MITRE ATT&CK-Matrix

Alle während der Emulation erkannten Prozessaktivitäten werden in Form einer MITRE ATT&CK-Matrix dargestellt.

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.



www.kaspersky.de