Kapersky Onderzoekssandbox

kaspersky BRING ON THE FUTURE

Sandboxtechnologieën

Sandboxtechnologieën zijn krachtige hulpmiddelen die het mogelijk maken om de herkomst van bestanden te onderzoeken, IOC's te verzamelen op basis van gedragsanalyse en kwaadaardige objecten te detecteren die niet eerder zijn ontdekt.

Kaspersky Onderzoekssandbox

Door een intelligente beslissing te nemen op basis van het gedrag van een bestand of URL en tegelijkertijd het procesgeheugen, de netwerkactiviteit, enz. te analyseren, is de optimale benadering om de geavanceerde, doelgerichte en op maat gemaakte bedreigingen van tegenwoordig te begrijpen.

Malware gebruikt tegenwoordig verschillende methoden om te voorkomen dat code wordt uitgevoerd als het daardoor als kwaadaardige activiteit wordt herkend. Als het systeem niet aan de vereiste parameters voldoet, vernietigt het kwaadaardige programma zichzelf waarschijnlijk, zonder sporen achter te laten. De kwaadaardige code kan alleen worden uitgevoerd als de sandboxing-omgeving normaal gedrag van eindgebruikers accuraat kan nabootsen.

Kapersky Onderzoekssandbox is een technologie waaraan we vanuit ons sandboxlaboratorium al een decennium ontwikkelen. Het omvat alle kennis over malwaregedrag die we hebben opgedaan tijdens ons continue dreigingsonderzoek, waardoor we elke dag meer dan 380.000 nieuwe schadelijke objecten detecteren. Deze krachtige technologie wordt op locatie geïmplementeerd en voorkomt dat gegevens op straat komen te liggen.

Het biedt een hybride aanpak, waarbij gedragsanalyse en solide anti-ontwijkingstechnieken worden gecombineerd met technologieën die menselijk gedrag simuleren. In Kaspersky Onderzoekssandbox kun je systeeminstallatiekopieën aanpassen aan echte omgevingen om de nauwkeurigheid van dreigingsdetectie en snelheid van het onderzoek te verhogen.

Hoofdkenmerken van het product:

- Geautomatiseerde objectanalyse in Windows-, Linux- en Android-omgevingen
- Dreigingsdetectie binnen Windows-systemen en -applicaties dankzij aangepaste installatiekopieën (alleen als ze op echte omgevingen zijn gebaseerd)
- De dreigingsscore op basis van statistieken en gegevens die worden verkregen tijdens het uitvoeren van een bestand, geeft het risiconiveau van het geanalyseerde object weer
- Implementatie op locatie voorkomt dat gegevens op straat komen te liggen
- Geavanceerde anti-ontwijkingstechnieken en technieken die menselijk gedrag nabootsen
- Handmatig indienen van bestand/URL en RESTful API
- Ondersteuning voor analyse van ruim 100 bestandstypen met gedetailleerde analyserapporten
- Aangepaste Suricata-regels om netwerkverkeer te scannen, kunnen worden toegevoegd aan en samen met de standaard Suricata-regels worden gebruikt
- Het product kan bare-metal geïmplementeerd worden en kan eenvoudig worden geschaald naar de vereiste prestaties

Overkoepelende architectuur van Kaspersky Onderzoekssandbox

Het product ondersteunt bare-metal-implementatie. De hardwareconfiguratie is afhankelijk van de vereiste prestaties en kan opgeschaald worden. Het vereist een netwerkverbinding van 100 Mbps voor elk kanaal en minimaal één onafhankelijke ISP-verbinding (twee of meer zijn aanbevolen voor fouttolerantie). De ISP moet op de hoogte zijn van en klaar zijn voor schadelijk verkeer.

Kaspersky Onderzoekssandbox is gebaseerd op een gepatenteerde propriëtaire technologie (patentnummer US10339301). Door de precieze voorwaarden na te spelen die het uitvoeren van malware triggeren, kunnen onderzoekers een verdacht bestand/verdachte URL in één keer analyseren.

Een kwaadaardig bestand kan, om blootstelling te voorkomen, eerst onderzoeken of het zich in een virtuele machine bevindt of kan inactief blijven tot de sandbox niet meer draait. In dergelijke gevallen versnelt de gepatenteerde technologie de tijd in de virtuele machine, zodat de kwaadaardige code wordt geforceerd om eerder uitgevoerd te worden.

Malware kan het kwaadaardige gedrag afgeschermd houden als die een specifieke applicatie wil aanvallen die ontbreekt in de sandbox. Onderzoekers nemen die uitdaging weg door logboeken te controleren, te begrijpen wat er ontbreekt en datgene aan een virtuele machine toe te voegen en het proces opnieuw uit te voeren. Als malware een bepaalde applicatie probeert te openen, onderschept het gepatenteerde systeem deze poging. Het wacht niet tot het uitvoeren van het bestand is voltooid, maar pauzeert het proces om de vereiste applicatie en de inhoud na te spelen.

Gedetailleerde analyserapporten

Als de analyse is voltooid, geeft de Onderzoekssandbox een gedetailleerd rapport over het gedrag en de functie van het geanalyseerde monster, waardoor jij de gewenste procedures kunt uitvoeren:

Samenvatting

Algemene informatie over het uitvoeren van een bestand/zoekresultaten van een URL.

Detectienamen

Een lijst van detecties (zowel AV en gedrag) die zijn geregistreerd tijdens het uitvoeren van het bestand.

Getriggerde netwerkregels

Een lijst van Suricata-netwerkregels die zijn getriggerd tijdens de analyse van het verkeer van het uitgevoerde object.

Uitvoermap

Een grafische reeksweergave van objectactiviteiten en de relatie ertussen.

Verdachte activiteiten

Verdachte activiteiten: een lijst met geregistreerde, verdachte activiteiten.

Schermafbeeldingen

Een set schermafbeeldingen die zijn gemaakt tijdens het uitvoeren van het bestand/het navigeren door URL's.

Ingeladen PE-afbeeldingen

Een lijst van ingeladen PE-afbeeldingen die zijn gedetecteerd tijdens het uitvoeren van bestanden/het navigeren door URL's

Bestandsbewerkingen

Een lijst van bestandsbewerkingen die zijn geregistreerd tijdens het uitvoeren van het bestand/het navigeren door URL's.

Registratiebewerkingen

Een lijst van bewerkingen die zijn uitgevoerd in het register van het besturingssysteem en zijn gedetecteerd tijdens het uitvoeren van het bestand/het navigeren door URL's.

Procesbewerkingen

Een lijst van bestandsinteracties met verschillende processen die zijn geregistreerd tijdens het uitvoeren van het bestand.

Synchronisatiebewerkingen

Een lijst met bewerkingen van aangemaakte synchronisatieobjecten (mutex, event, semaphore) die zijn geregistreerd tijdens het uitvoeren van het bestand/het navigeren door URL's.

Gedownloade bestanden

Een lijst van bestanden geëxtraheerd uit het netwerkverkeer tijdens het uitvoeren van het bestand/het navigeren door URL's.

Opgeslagen bestanden

Een lijst van bestanden die zijn opgeslagen (aangemaakt of aangepast) door het uitgevoerde bestand.

HTTPS/HTTP/DNS/IP/TCP/UDP en meer

Details van netwerksessies/-verzoeken die zijn opgenomen tijdens het uitvoeren van het bestand/het navigeren door URL's.

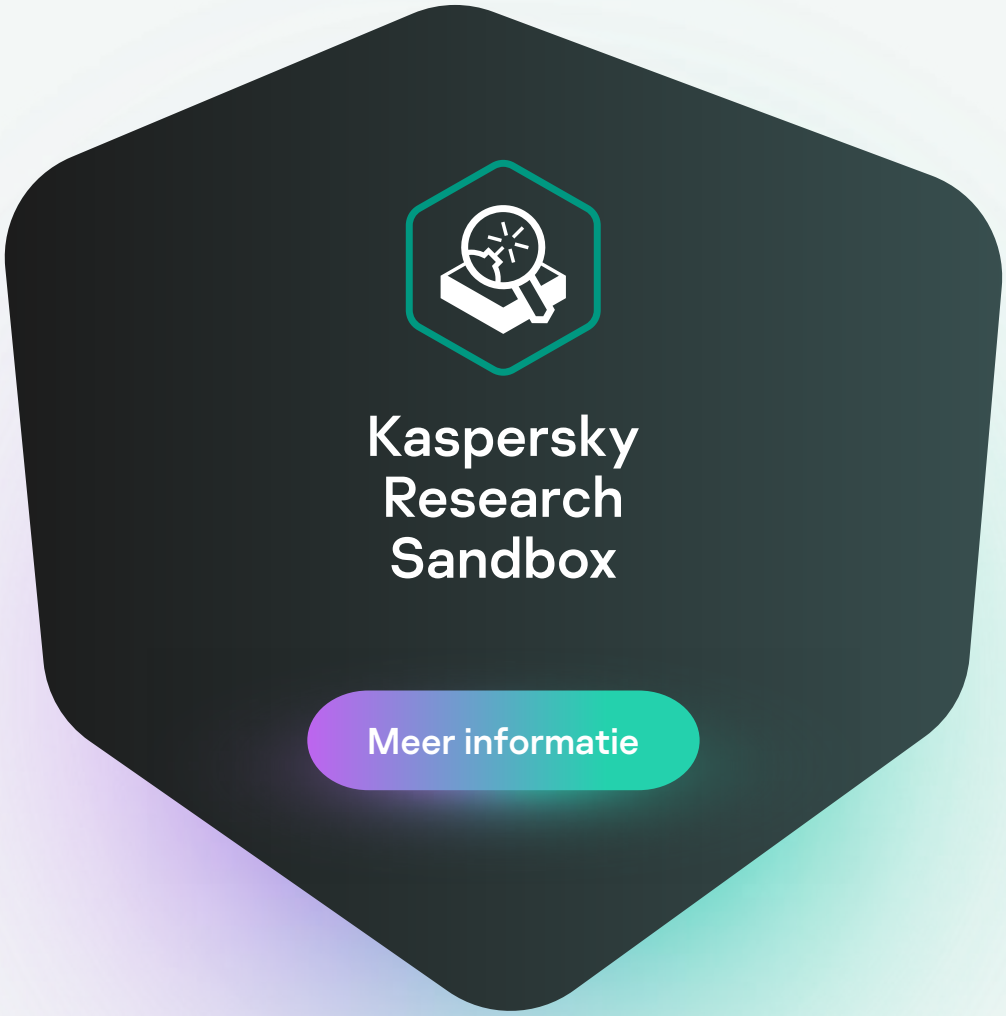
Dump van netwerkverkeer (PCAP)

Netwerkactiviteit kan in PCAP-formaat worden gedownload.

MITRE ATT&CK-matrix

Alle geïdentificeerde procesactiviteiten die tijdens de emulatie zijn opgenomen, worden weergegeven in de vorm van een MITRE ATT&CK-matrix.

Kaspersky Onderzoekssandbox is de voorkeurstool om onbekende dreigingen te detecteren. Het is een meer volwassen product en heeft meer focus op complexe dreigingen dan elke andere oplossing.



www.kaspersky.nl