kaspersky BRING ON THE FUTURE

Kaspersky Threat Attribution Engine

Die Überwachung, Analyse, Interpretation und Abwehr der sich ständig weiterentwickelnden IT-Sicherheitsbedrohungen ist mit immensem Aufwand verbunden. Threat Intelligence geht weit über den aktuellen Hype einer aufkommenden Nische in der Informationssicherheitsbranche hinaus. Der größte Streitpunkt, aber zugleich auch das größte Interesse innerhalb der Bedrohungsanalyse, kommt hierbei der Threat Attribution zu.

Vorteile des Produkts im Überblick:

- Unverzögerter Zugang zu einem Repository an kuratierten Daten zu Hunderten von APT-Akteuren und Beispieldaten
- Möglichkeit zur effizienten automatisierten oder manuellen Priorisierung von Bedrohungen und Warnhinweisen
- Möglichkeit zur Eingabe von privaten Akteuren und Beispieldaten, damit das Produkt lernt, Daten zu erkennen, die Dateien in Ihrer privaten Sammlung ähnlich sind
- Manueller Daten-Upload und offene API zur Integration in automatisierte Workflows
- Kann in sicheren Air-Gap-Umgebungen angewendet werden, um Ihre Systeme und Daten zu schützen und alle Compliance-Anforderungen zu erfüllen
- Absolute Vertraulichkeit und Privatsphäre bei allen Einsendungen, damit sensible Informationen nicht offen gelegt werden

Und dafür gibt es gute Gründe. Die durchschnittliche Zeit von der Erkennung hoch entwickelter Bedrohungen bis zur Reaktion ist aufgrund komplexer Untersuchungs- und Reverse Engineering-Prozesse in der Regel zu lang. In vielen Fällen reicht sie den Angreifern aus, um ihre Ziele zu erreichen. Eine korrekte und zeitnahe Zuordnung hilft nicht nur die Reaktionszeiten von Stunden auf Minuten zu verkürzen, sondern auch die Zahl der Fehlalarme zu reduzieren.

Die Identifizierung eines zielgerichteten Angriffs, die Erstellung eines Angreiferprofils und der entsprechenden Zuordnungsfaktoren für die einzelnen Bedrohungsakteure ist ein langer Prozess, der mitunter sogar Jahre dauern kann. Für eine funktionierende Zuordnung braucht man große Mengen von über die Jahre gesammelten Daten sowie ein hoch qualifiziertes Team von Forschern mit einschlägiger Erfahrung. Dazu verfolgen Forscher meist die Aktivitäten unterschiedlicher Gruppen und füttern ihre Datenbank stetig mit Informationen. Diese Datenbank wird irgendwann zu einer wertvollen Ressource, die als Tool freigegeben werden kann.

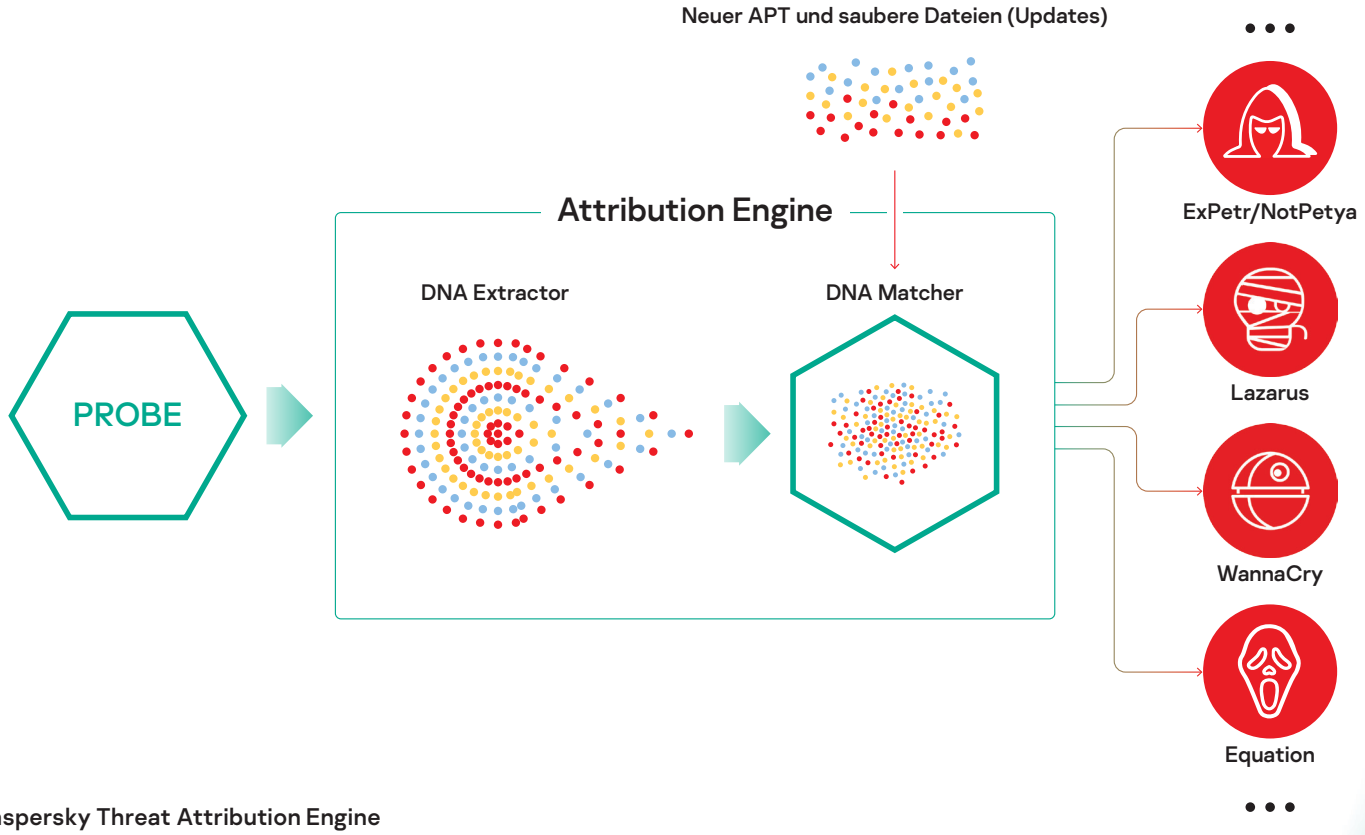
Die Kaspersky Threat Attribution Engine umfasst eine Datenbank mit APT-Malware-Proben und „sauberen" Dateien, die von Kaspersky-Experten in den letzten 22 Jahre gesammelt wurden. Wir verfolgen mehr als 600 Bedrohungsakteure und -Kampagnen mit mehr als 120 APT Intelligence Reports, die jedes Jahr veröffentlicht werden. Mit fortwährender Forschung halten wir unsere große APT-Sammlung mit mehr als 60 000 Dateien auf dem neuesten Stand. Dank dieses Bestands lassen sich Fehlalarme vermeiden und die Zuordnung erfolgt dank automatisierter Tools wesentlich präziser.

In einem einzigartigen Verfahren werden Proben auf Ähnlichkeiten hin überprüft, während die Zahl der False Positives bei nahezu Null gehalten wird. Das Produkt kann neue Angriffe mit bekannter APT-Malware, vorangegangenen Angriffen und Hackern in Verbindung bringen, so dass Bedrohungen mit hohem Risiko unter der Vielzahl der weniger schwerwiegenden Vorfällen erkennbar werden. So können zeitnah Schutzmaßnahmen getroffen werden, um Angreifer daran zu hindern, in das System einzudringen.

Funktionsweise

Die Kaspersky Threat Attribution Engine analysiert die „DNA" von Malware und sucht dabei automatisiert nach Ähnlichkeiten mit dem Code und den involvierten Akteuren von zuvor untersuchten APT-Beispieldaten. Sie vergleicht die „Genotypen", d. h. kleine binäre Bestandteile der zerlegten Dateien, mit Datenproben aus der APT-Malware-Datenbank. Im Ergebnis erhält man einen Bericht zum Ursprung der Malware, den Bedrohungsakteuren sowie den Ähnlichkeiten mit bekannten APT-Dateien.Außerdem bietet das Produkt Sicherheitsteams die Möglichkeit, private Akteure und Objekte zur Datenbank hinzuzufügen, damit das Produkt lernt, Daten zu erkennen, die den Dateien in Ihrer privaten Sammlung ähnlich sind. Mit der Threat Attribution Engine ist die Zuordnung verglichen zu den Jahren, die sie in der Vergangenheit in Anspruch genommen hat, innerhalb von Sekunden erledigt.

Die Threat Attribution Engine kann in einer sicheren, isolierten Umgebung bereitgestellt werden, in der Dritte nur eingeschränkten Zugang zu den verarbeiteten Informationen und den eingesendeten Objekten haben. Es gibt eine API, um die Engine mit anderen Tools und Frameworks zu verbinden, damit die Zuordnungsfunktion in bestehende Infrastrukturen und automatisierte Prozesse eingegliedert werden kann.



Kaspersky Threat Attribution Engine

Detaillierte Informationen zum zugehörigen APT-Akteur findet man in den Kaspersky APT Intelligence Reports[1]. Als Abonnent von Kaspersky APT Intelligence Reporting erhalten Sie exklusiven Zugang zu unseren Forschungsergebnissen und Erkenntnissen, einschließlich der vollständigen technischen Details in unterschiedlichen Formaten zu jedem APT, noch während dieser aufgedeckt wird – inklusive aller Bedrohungen, die nie veröffentlicht werden.

Die Kaspersky Threat Attribution Engine ergänzt und stärkt das Kaspersky-Portfolio für nationale Cybersicherheitsbehörden und kommerzielle Security Operations Centers (SOCs), indem es sie bei der Einführung effektiver Verfahren zum Umgang mit Sicherheitsvorfällen unterstützt.

Die Kaspersky Attribution Engine bietet SOCs wesentliche Unterstützung bei deren Bemühungen:

- Dateien schnell bekannten APT-Akteuren zuzuordnen, um Motivation, Methodik und Tools hinter den Cybervorfällen aufzudecken;
- schnell zu ermitteln, ob Sie das primäre Ziel eines Angriffs oder eher zufällig betroffen sind, um entsprechende Maßnahmen zur Eindämmung einzuleiten;
- Bedrohungen effektiv und zeitnah abzuschwächen, indem aus dem Kaspersky APT Intelligence Reporting auch praktisch umsetzbare Threat Intelligence zur APT-Familie hinzugezogen wird.

1 Ein Abonnement von Kaspersky APT Intelligence Bericht kann separat käuflich erworben werden

Neues über Cyberbedrohungen: https://de.securelist.com/
IT-Sicherheitsnachrichten: https://www.kaspersky.de/blog/b2b/
IT-Sicherheit für KMUs: kaspersky.de/business
IT-Sicherheit für Großunternehmen: kaspersky.de/enterprise

www.kaspersky.de

Beständigkeit, Unabhängigkeit und Transparenz – das zeichnet uns aus. Wir möchten eine sicherere Welt schaffen, in der Technologien uns das Leben erleichtern. Deshalb schützen wir sie, 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.