kaspersky BRING ON THE FUTURE

Kaspersky Threat Attribution Engine

Jatkuvasti muuttuvien tietoturvauhkien seuraaminen, tulkitseminen ja hallinta vaatii paljon työtä. Uhkatiedot ovat paljon enemmän kuin paljon puhuttu uusi markkinarako tietoturva-alalla, ja uhkien määritys on todennäköisesti huomattavin niihin liittyvä kiinnostuksen kohde ja kiistanaihe.

Tuotteen kohokohdat:

- Satojen APT-toimijoiden ja -näytteiden kuratoidut tiedot heti käytettävissä
- Mahdollistaa tehokkaan automatisoidun tai manuaalisen uhkien priorisoinnin ja hälytysten luokittelun
- Toiminnot, joilla voi lisätä omia tekijöitä ja näytteitä sekä opettaa tuotetta havaitsemaan näytteitä, jotka ovat samanlaisia kuin yksityisissä kokoelmissasi olevat
- Manuaalinen näytteiden lataus ja avoin ohjelmointirajapinta integrointiin automatisoituihin työnkulkuihin
- Voidaan ottaa käyttöön suojatuissa, tiiviissä ympäristöissä järjestelmien ja tietojen suojaamiseksi sekä säännöstenmukaisuusvaatimusten noudattamiseksi
- Kaikki lähetetyt tiedot pysyvät ehdottoman yksityisinä ja luottamuksellisina, jotta arkaluonteiset tiedot eivät paljastu

Siihen on myös selvä syy. Keskimääräinen aika kehittyneiden uhkien havaitsemisesta reagointiin on liian pitkä, mikä johtuu monimutkaisista tutkimuksista ja takaisinmallinnusprosesseista. Monissa tapauksissa hyökkääjät ehtivät saavuttaa tavoitteensa. Oikeanlainen ja hyvin ajoitettu määritys sekä lyhentää häiriötapausten reagointiajan tunneista minuutteihin että vähentää vääriä osumia.

Kohdistetun hyökkäyksen tunnistaminen, hyökkääjien profilointi ja eri uhkatoimijoiden määritystekijöiden laatiminen on pitkä ja perusteellinen tehtävä, joka saattaa kestä vuosia. Lisäksi toimivan määrityksen laatimiseen tarvitaan kerättyjä tietoja usean vuoden ajalta ja taitava tutkimustiimi, jolla on kokemusta tutkinnasta. Tavallisesti tutkijat seuraavat eri ryhmien toimintaa ja lisäävät tiedot tietokantaan. Tällainen tietokanta on arvokas resurssi, joka voidaan jakaa työkaluna.

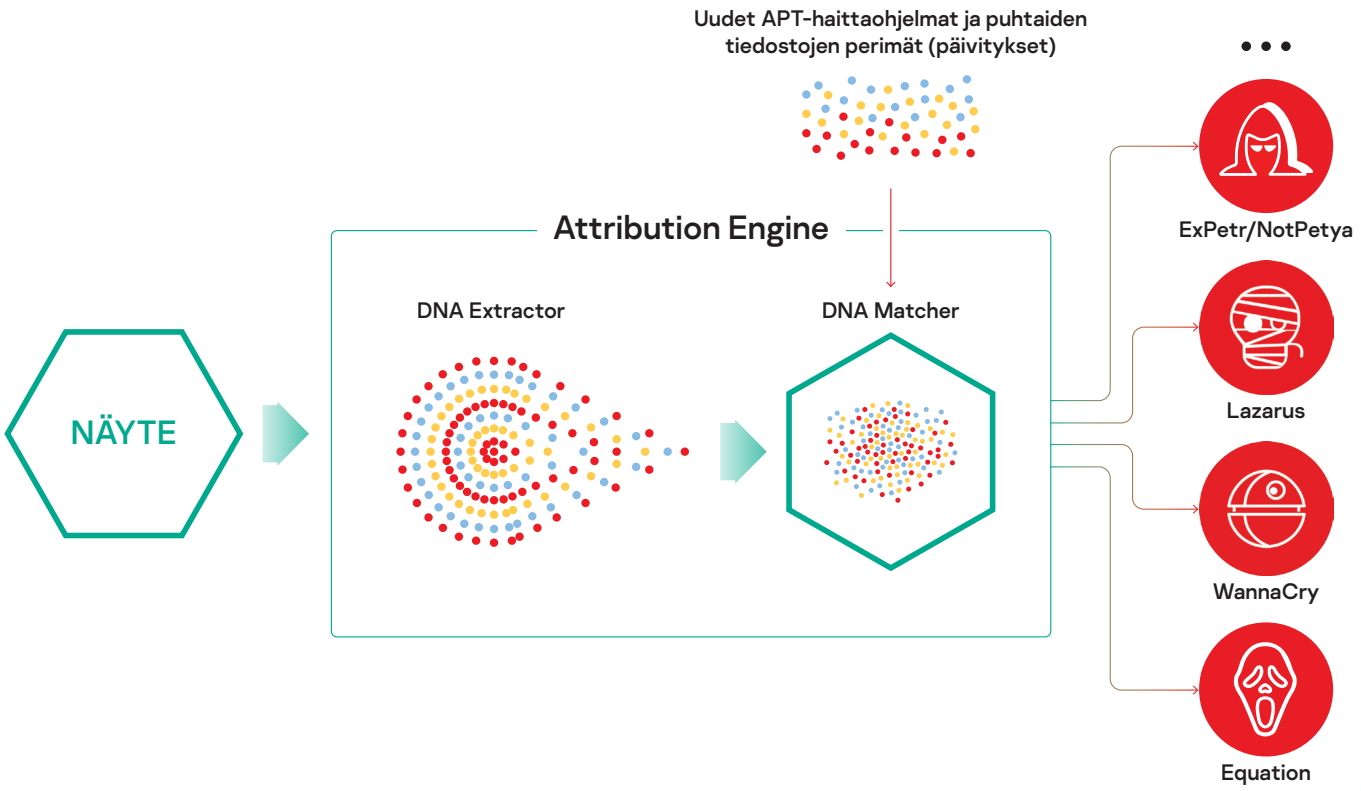
Kaspersky Threat Attribution Engine sisältää APT-haittaohjelmanäytteiden tietokannan ja Kasperskyn asiantuntijoiden yli 22 vuoden ajalta keräämät puhtaat tiedostot. Seuraamme yli 600:tta APT-toimijaa ja -kampanjaa ja vuosittain julkaistavissa yli 120:ssä APT Intelligence -raportissa. Jatkuva tutkimuksemme pitää ajan tasalla laajaa APT-kokoelmaa, joka sisältää yli 60 000 tiedostoa. Se parantaa väärien osumien tunnistusta ja tarkentaa määritystä automatisoiduilla työkaluilla.

Tuotteen avulla voidaan ainutlaatuisesti verrata näytteiden samankaltaisuutta ja samalla varmistaa, että vääriä osumia ei tule. Se pystyy yhdistämään uuden hyökkäyksen nopeasti tunnettuun APT-haittaohjelmaan, aiempiin kohdistettuihin hyökkäyksiin ja hakkeriryhmiin. Siten voidaan erottaa suurimmat uhkat vähemmän vakavista tapahtumista ja ryhtyä oikea-aikaisiin suojaustoimiin, jotta hyökkääjä ei pysty kaappaamaan järjestelmää.

Toiminta

Kaspersky Threat Attribution Engine analysoi automaattisesti haittaohjelmien "genetiikkaa" etsien koodia, joka muistuttaa aiemmin tutkittuja APT-näytteitä ja niihin liittyviä toimijoita. Se vertaa "perimää" eli purettujen tiedostojen pieniä binaariosia APT-haittaohjelmanäytteiden tietokantaan ja ilmoittaa haittaohjelman alkuperän, uhkatoimijat ja tiedostojen samankaltaisuuden suhteessa tunnettuihin APT-näytteisiin. Lisäksi tietoturvatiimit voivat lisätä tuotteen avulla omia tekijöitä ja kohteita sen tietokantaan ja opettaa tuotetta havaitsemaan näytteitä, jotka ovat samanlaisia kuin yksityisessä kokoelmassasi olevat tiedostot. Threat Attribution Engine -tuotteella määritys kestää vain muutaman sekunnin, kun aiemmin siihen kului useita vuosia.

Tuotteen voi ottaa käyttöön suojatussa, tiiviissä ympäristössä, jossa kolmannet osapuolet eivät pääse käsiksi käsiteltyihin tietoihin ja lähetettyihin kohteisiin. Käytettävissä on ohjelmointirajapinta, jolla Enginen voi yhdistää muihin työkaluihin ja puitteisiin, jotta määritys voidaan ottaa käyttöön nykyisissä infrastruktuureissa ja automatisoiduissa prosesseissa.



Kaspersky Threat Attribution Engine

Yksityiskohtaiset tiedot vastaavasta APT-toimijasta ovat Kaspersky APT Intelligence -raporteissa[1]. Kaspersky APT Intelligence Reporting -tilaajana saat ainutlaatuisen jatkuvan pääsyn tutkimuksiimme ja havaintoihimme, kuten kunkin APT-haittaohjelman täydellisiin teknisiin tietoihin useassa muodossa heti, kun tiedot on saatu selville. Tämä koskee myös kaikkia uhkia, joita ei julkisteta lainkaan.

Kaspersky Threat Attribution Engine laajentaa ja vahvistaa Kasperskyn tuotevalikoimaa entisestään kansallisia kybersuojaustoimijoita ja kaupallisia tietoturvavalvomoita (SOC) varten tukien niitä tehokkaan häiriöiden hallintaprosessin laadinnassa.

Kaspersky Attribution Engine tehostaa suojaustoimintoja merkittävästi ja helpottaa

- tiedostojen nopeaa yhdistämistä tunnettuihin APT-toimijoihin kybertapahtumien taustalla olevien vaikuttimien, menetelmien ja työkalujen selvittämiseksi,
- nopeaa arviointia hyökkäyksen todellisesta kohteesta, jotta voidaan määrittää asianmukaiset eristämis- ja vastaustoimet,
- tehokkaan ja oikea-aikaisen uhkien hallinnan varmistamista Kaspersky APT Intelligence Reporting -palvelusta saatujen käyttökelpoisten APT-haittaohjelmaperhettä koskevien uhkatietojen avulla.

1 Kaspersky APT Intelligence Reporting -tilaus on ostettava erikseen

Kyberuhkauutisia: www.securelist.com
Tietoturvauutisia: business.kaspersky.com
PK-yritysten tietoturva: kaspersky.com/business
Suuryritysten tietoturva: kaspersky.com/enterprise

www.kaspersky.com

© 2020 AO Kaspersky Lab
Rekisteröidyt tavara- ja palvelumerkit ovat niiden omistajien omaisuutta.

Toimimme varmasti. Toimimme itsenäisesti. Toimimme läpinäkyvästi. Olemme sitoutuneet rakentamaan turvallisempaa maailmaa, jossa tekniikka parantaa elämänlaatua. Siksi haluamme suojata sen, jotta kaikilla kaikkialla olisi samat rajattomat mahdollisuudet. Kybersuojaus takaa turvallisemman tulevaisuuden.

Lisätietoja: kaspersky.com/transparency

Proven.
Transparent.
Independent.