Kaspersky Threat Data Feeds

kaspersky bring on the future

Kaspersky Threat Data Feeds

Kaspersky Threat Data Feeds

Gli attacchi informatici possono verificarsi ogni giorno. Le minacce informatiche continuano a crescere in termini di frequenza, complessità e livello di offuscamento, nel tentativo di compromettere le soluzioni di protezione. Gli autori degli attacchi usano complicate kill chain, campagne oppure tattiche, tecniche e procedure (TTP) personalizzate per bloccare i processi aziendali o danneggiare i clienti. Emerge in tutta evidenza la necessità di adottare nuovi metodi di protezione, basati sulla threat intelligence.

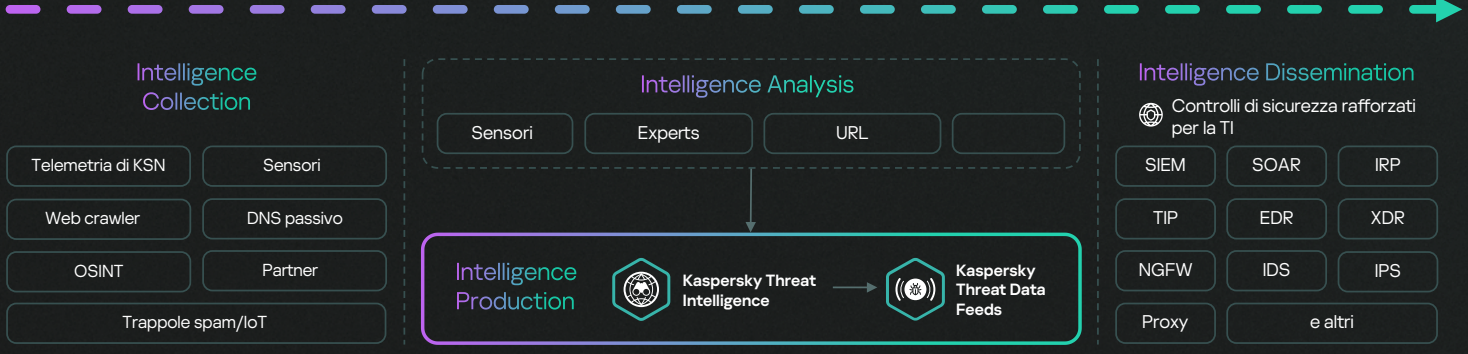
Integrando nei sistemi di sicurezza esistenti, come ad esempio i sistemi SIEM, SOAR e le piattaforme di Threat Intelligence, feed di Threat Intelligence aggiornati, contenenti informazioni su IP, URL e hash di file sospetti e pericolosi, i team di sicurezza possono automatizzare il processo di triage iniziale e fornire ai relativi specialisti il contesto necessario per identificare immediatamente gli avvisi che richiedono analisi approfondite o che vanno inoltrati ai team di incident response per ulteriori indagini e risposte.

Dati contestuali

Le voci nei feed forniti da Kaspersky contengono i dati contestuali che consentono rapidamente di confermare le minacce e definire le priorità:

- Nome della minaccia
- Indirizzi IP e nomi di dominio di risorse Web dannose
- Hash di file dannosi
- Oggetti vulnerabili e compromessi
- Tattiche, tecniche e procedure di attacco secondo la classificazione MITRE ATT&CK
- Timestamp
- Geolocalizzazione
- Popolarità e così via

Come funziona



I feed di dati sulle minacce di Kaspersky vengono aggregati da fonti altamente affidabili ed eterogenee:

Kaspersky Security Network

Sofisticata infrastruttura cloud che raccoglie e analizza i dati anonimi sulle minacce informatiche di oltre 400 milioni di volontari in tutto il mondo per fornire la risposta più rapida alle nuove minacce sfruttando l'analisi di Big Data, il machine learning e le competenze umane.

Web crawler

Raccogliete nuovi campioni di malware e legittimi da svariate fonti: OSINT, ricerche degli analisti Kaspersky e i nostri sistemi automatici di elaborazione e analisi che estraggono gli URL dal malware.

BotFarm

Un team di ricerca dedicato alle botnet estrae le configurazioni dei bot, esegue il reverse engineering dei loro protocolli di comunicazione e monitora i comandi dei centri di comando per ottenere preziose informazioni sulle minacce.

Esche di spam

Ogni anno i nostri sistemi anti-phishing prevengono più di 500 milioni di clic su link di phishing e bloccano più di 160 milioni di allegati e-mail dannosi, da cui estraiamo ulteriori informazioni che vanno ad arricchire i nostri flussi di dati.

Partner

Partecipiamo a partnership per condividere campioni di malware con altri fornitori e organizzazioni di cybersecurity.

Sensori

Honeypot, sinkhole e altri metodi di intercettazione degli attacchi ITW, ad esempio dispositivi IoT, sistemi vulnerabili, software e così via. Gli analisti Kaspersky ricercano i tentativi di attacco e i metodi degli aggressori, estraggono gli indicatori di compromissione e li collegano ad altre fonti di dati.

DNS passivo

I dati vengono raccolti a livello globale da terze parti attendibili, come organizzazioni di hosting e provider di servizi Internet.

OSINT

I dati sugli avversari vengono raccolti automaticamente da fonti pubbliche, quali testate giornalistiche, social media, report pubblici, Dark Web e così via. Utilizziamo questi dati per cercare nuovi campioni dannosi esplorando l'infrastruttura dell'avversario e aggiungendoli continuamente alla nostra Knowledge Base.

Ogni indicatore rilevato viene sottoposto a un processo di screening in più fasi in un sistema di elaborazione automatizzato che utilizza tecnologie di analisi della fiducia e della reputazione e modelli di machine learning addestrati su campioni di centinaia di milioni di file affidabili e dannosi per eliminare i falsi positivi. Ogni indicatore viene inoltre analizzato in più sandbox, da cui vengono estratti decine di attributi aggiuntivi come TTP, comportamento della rete, comportamento del sistema operativo e una serie di altre relazioni.

Tutto questo fa di Kaspersky Threat Intelligence una preziosa fonte di informazioni di livello tattico in grado di rafforzare i centri di monitoraggio delle minacce e di rilevare gli avversari in prima linea nell'organizzazione.

Caratteristiche principali

I feed di dati vengono generati automaticamente in tempo reale sulla base dei risultati in tutto il mondo, fornendo tassi di rilevamento e precisione elevati.

La facilità di implementazione è garantita da documentazione supplementare, esempi specifici, un account manager tecnico dedicato e l'avanzato supporto tecnico di Kaspersky, che si combinano perfettamente tra loro, consentendo un'agevole e immediata integrazione.

Formati di diffusione semplici e leggeri (JSON, CSV, OpenIoC, STIX) tramite HTTPS, TAXII o appositi meccanismi di distribuzione, supportano in modo efficiente la semplice integrazione dei feed nelle soluzioni di sicurezza. I sistemi SIEM e le piattaforme TI principali sono completamente supportati.

I feed di dati costellati di falsi positivi sono sostanzialmente inutili. Per questo motivo, prima del rilascio dei feed, vengono applicati test estesi e appositi filtri, al fine di garantire la fornitura di dati controllati al 100%.

Centinaia di esperti contribuiscono alla generazione dei feed, tra cui analisti di sicurezza situati in tutto il mondo, i rinomati esperti di sicurezza dei team GReAT e dei team che operano in ambito R&S. I responsabili della sicurezza ricevono informazioni critiche e alert generati da dati di massima qualità, senza alcun rischio di essere travolti da una valanga di indicatori e alert inutili.

Tutti i feed sono generati e monitorati da un'infrastruttura ad alta tolleranza di errore, assicurando disponibilità continua.

Vantaggi

1. Rafforzamento delle soluzioni implementate per la difesa della rete aziendale, inclusi SIEM, firewall, NGFW, IPS/IDS, proxy per la sicurezza, soluzioni DNS, anti-APT, con Indicatori di Compromissione (IoC) continuamente aggiornati e contestualizzati, per offrire informazioni approfondite sugli attacchi informatici e fornire una maggiore comprensione delle intenzioni, delle capacità e degli obiettivi degli avversari.

2. Miglioramento e accelerazione dell'incident response e delle capacità forensi automatizzando il processo di triage iniziale, fornendo agli analisti di sicurezza un contesto sufficiente per identificare immediatamente gli alert che devono essere indagati o inoltrati ai team di incident response per ulteriori indagini.

3. Prevenzione dell'esfiltrazione delle risorse sensibili e delle proprietà intellettuali dalle macchine infette verso l'esterno dell'organizzazione. Rilevate rapidamente le risorse infette per proteggere la reputazione del brand, mantenendo il vantaggio competitivo e tutelando le opportunità aziendali.

4. In qualità di MSSP, è possibile far crescere l'azienda grazie a una Threat Intelligence leader di settore offerta ai clienti come servizio premium.

5. Da parte loro, i CERT hanno l'opportunità di potenziare ed estendere considerevolmente le capacità di detection e identificazione delle minacce informatiche.

Kaspersky Threat Intelligence

Kaspersky Threat Intelligence consente di accedere a un'ampia gamma di informazioni raccolte dai nostri analisti e ricercatori di livello mondiale. Questi dati aiuteranno l'organizzazione a contrastare efficacemente le odierne minacce informatiche.

La nostra azienda possiede una conoscenza approfondita, una vasta esperienza nella ricerca sulle cyberminacce e informazioni dettagliate su tutti gli aspetti della cybersecurity, che le consentono di fornire dati aggiornati sulle minacce tattiche, operative e strategiche.
Questo ci ha reso un partner affidabile delle forze dell'ordine e delle organizzazioni governative di tutto il mondo, tra cui l'Interpol e diverse unità CERT. Tutto questo è disponibile sotto forma di dati rilevanti e fruibili attraverso Kaspersky Threat Intelligence Portal.

Kaspersky Threat Intelligence

Ulteriori informazioni

www.kaspersky.it

© 2024 AO Kaspersky Lab.
I marchi registrati e i marchi di servizio appartengono ai rispettivi proprietari.

#kaspersky
#bringonthefuture