Kaspersky Network Security Threat Data Feeds

kaspersky bring on the future

La protezione degli endpoint non basta.

È necessaria anche la protezione a livello di rete.

Ecco perché:

- La protezione da tipi di attacchi diversi deve coprire più livelli
- Non tutti gli host dell'ambiente disporranno della protezione della sicurezza degli endpoint, ad esempio non tutti i server business-critical o gli host di una rete industriale.
- Alcuni host "protetti" potrebbero non essere aggiornati con le firme, gli hash e le regole di rilevamento più recenti.

Kaspersky Network Security Threat Data Feeds

Oggi quasi tutte le aziende dispongono di un Next-Generation Firewall (NGFW). Incrementa i livelli di protezione delle reti aziendali contro i cyberattacchi ed è quindi uno dei moderni controlli di sicurezza di rete più efficaci.

La maggior parte degli NGFW non solo è in grado di utilizzare le conoscenze interne sulle cyberminacce, ma offre anche funzionalità che consentono di usare elenchi dinamici di indicatori di compromissione (IoC) provenienti da fonti esterne per bloccare le cyberminacce in tempo reale.

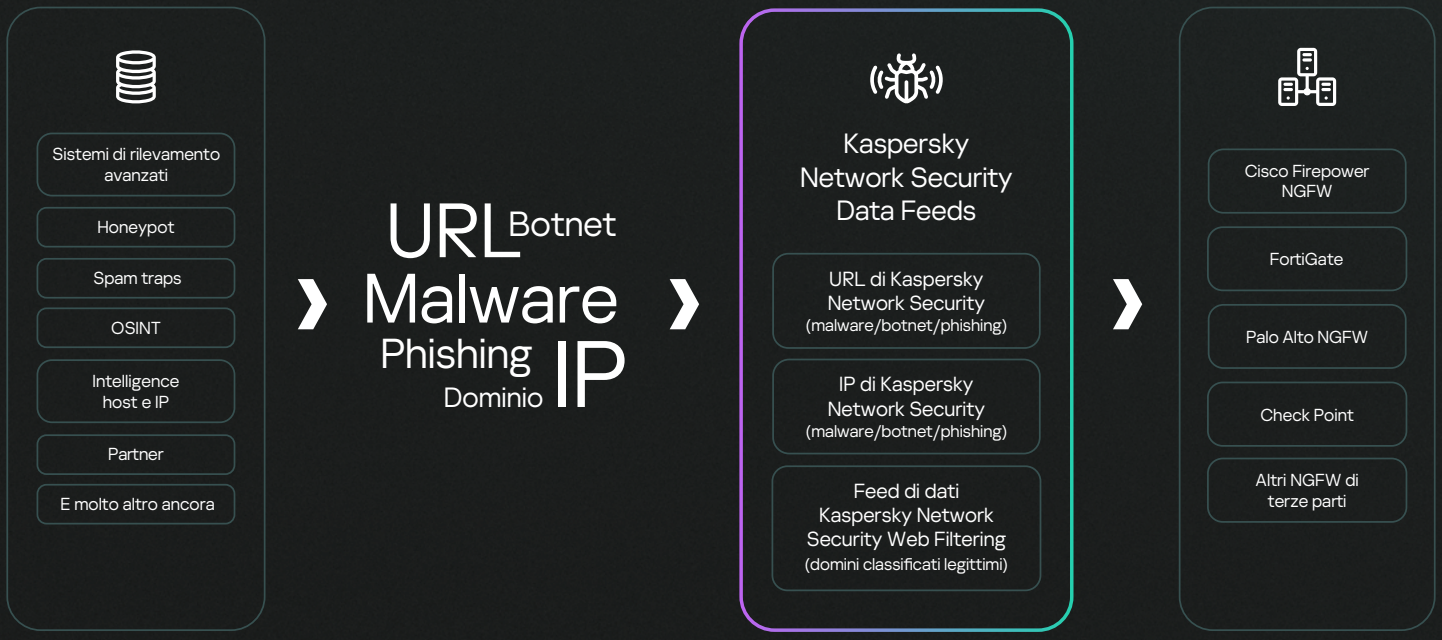
Configurare rapidamente le regole di rilevamento NGFW per essere sempre un passo avanti rispetto agli avversari è quasi impossibile. Ecco perché la conoscenza delle minacce esterne è fondamentale. Fornisce infatti un ulteriore elemento di protezione essenziale per l'ambiente, che altrimenti potrebbe sfuggire.

Kaspersky offre raccolte di IoC appositamente create che, se importate in un NGFW, migliorano significativamente il livello di protezione della rete aziendale dalle minacce più diffuse, senza complicate integrazioni o configurazioni e mantenendo la topologia di rete attuale.

I feed di dati sulle minacce di Kaspersky Network Security si basano su Kaspersky Threat Intelligence Data Feeds e contengono elenchi regolarmente aggiornati di diversi tipi di IoC (indirizzi IP e domini). L'utilizzo di queste informazioni consente di monitorare/bloccare l'accesso degli utenti a risorse di rete pericolose.

Per saperne di più

Integrazioni di Kaspersky Network Security Data Feeds



Raccolta ed elaborazione dei dati

I feed di dati di Kaspersky Network Security sono composti da più elenchi, ognuno dei quali riguarda un tipo specifico di cyberminaccia. I feed contengono gli elenchi degli indirizzi IP con la percentuale netta di minacce più elevata e i domini di primo e secondo livello delle risorse note per distribuire malware, agire come centri di comando e controllo (C&C) di botnet o ospitare risorse di phishing.

I feed di dati vengono aggregati da fonti altamente affidabili ed eterogenee, quali Kaspersky Security Network e i nostri Web crawler proattivi, il servizio di monitoraggio botnet (monitoraggio 24 ore su 24, 7 giorni su 7, 365 giorni all'anno di botnet e delle relative attività e obiettivi) e servizi di intelligence host e IP.

Tutti i dati aggregati vengono accuratamente ispezionati in tempo reale e perfezionati tramite diverse tecniche di rielaborazione, quali criteri statistici, sandbox, motori euristici, strumenti di similarità, profilatura del comportamento, convalida da parte degli analisti e verifica delle liste consentiti:

Caratteristiche principali

Aggiornamenti in tempo reale

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

Kaspersky Security Network fornisce visibilità su una percentuale significativa di tutto il traffico Internet, coprendo decine di milioni di utenti finali in oltre 213 paesi

Supporto nativo

Supporto nativo per i NGFW più diffusi:

- Cisco
- FortiGate
- Palo Alto
- Altri NGFW di terze parti (con la funzionalità degli elenchi dinamici esterni con supporto di autenticazione di base)

Autenticazione sicura

I feed di dati offrono una serie di metodi di autenticazione personalizzati per soddisfare le diverse esigenze di sicurezza e preferenze di integrazione.

Facile integrazione

Le dettagliate guide supplementari per ogni NGFW supportato e il team tecnico di Kaspersky consentono una facile configurazione e forniscono un valore immediato

Disponibilità continua

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

Dati verificati al 100%

I feed di dati disseminati di falsi positivi sono dannosi perché possono bloccare risorse legittime.

I feed di dati di Kaspersky Security Network applicano test estesi e appositi filtri, al fine di garantire la fornitura di dati controllati al 100%

Vantaggi

Rinforzare le soluzioni di difesa della rete

con IOC continuamente aggiornati per bloccare automaticamente le cyberminacce più diffuse

Impedire la fuga di informazioni sensibili

e di proprietà intellettuale da computer infetti all'esterno dell'organizzazione

Bloccare rapidamente le cyberminacce per proteggere

l'organizzazione e mantenere la continuità aziendale

Kaspersky Threat Data Feeds

Per saperne di più

www.kaspersky.it

#kaspersky
#bringonthefuture