KASPERSKY lab

KASPERSKY PRIVATE SECURITY NETWORK: THREAT INTELLIGENCE IN TEMPO REALE, ALL'INTERNO DELL'INFRASTRUTTURA AZIENDALE

Threat intelligence globale per implementazione locale

www.kaspersky.it

UN LABORATORIO DELLE MINACCE BASATO SU CLOUD PER CLIENTI KASPERSKY LAB

Dal 2008, la threat Intelligence basata su cloud di Kaspersky Lab (Kaspersky Security Network) ha fornito dati sulla reputazione in tempo reale e informazioni sulle minacce a milioni di clienti in tutto il mondo. Utilizzando dati resi anonime provenienti da 80 milioni di sensori degli endpoint al mondo, tutti i file che passano attraverso i sistemi protetti da Kaspersky Lab vengono analizzati utilizzando la più pertinente threat intelligence.

Le soluzione standard per la sicurezza impiegano fino a quattro ore per ricevere le informazioni necessarie a rilevare e bloccare gli oltre 360.000 programmi nocivi rilevati quotidianamente dai ricercatori di Kaspersky Lab. La condivisione dell'intelligence sulle minacce tramite Kaspersky Private Security Network fornisce queste informazioni in 30-40 secondi, senza uscire dall'organizzazione.

Mentre tutte le informazioni elaborate da Kaspersky Security Network vengono rese completamente anonime e dissociate dalla loro origine, Kaspersky Lab riconosce che alcune organizzazioni, per motivi di conformità o di politica aziendale, richiedono l'assoluto blocco dei dati. Da sempre questo ha significato che le aziende non si sono avvalse dei servizi di sicurezza basati sul cloud.

Per questi clienti, Kaspersky Lab ha sviluppato un prodotto completo: **Kaspersky Private Security Network** consente alle aziende di sfruttare la maggior parte dei vantaggi della threat intelligence globale basata su cloud senza divulgare alcun dato al di fuori del perimetro controllato. Questo è tutto: si tratta di una versione di Kaspersky Security Network personale, locale e completamente privata dell'azienda.

Per comprendere come funziona Kaspersky Private Security Network, diamo prima un'occhiata a Kaspersky Security Network.

Kaspersky Security Network è disponibile come opzione, come componente aggiuntivo delle soluzioni Kaspersky Enterprise Security for Business, Kaspersky Security for Virtualization, Kaspersky Security for Storage, Kaspersky Security for Data Centers, Kaspersky Anti-APT e Kaspersky Fraud Prevention.

THREAT INTELLIGENCE IN TEMPO REALE FORNITA DAL CLOUD

Kaspersky Security Network (KSN) utilizza le elevate prestazioni del cloud per garantire il più veloce rilevamento delle minacce e i più rapidi tempi di risposta. Informazioni "on-the-fly" sulle più recenti minacce vengono inviate al cloud protetto per l'analisi; ogni volta che un sistema protetto da Kaspersky Lab rileva un file, un'applicazione o un sito web sospetto, questo può essere confrontato con le informazioni sulle minacce basate su cloud e il verdetto sulla sicurezza viene fornito immediatamente. In genere, le tecniche convenzionali impiegano ore per aggiornare i database con nuove informazioni sulle minacce, mentre il sistema o l'analisi delle minacce locali consuma risorse.

Contribuire a un maggiore livello di sicurezza

Ogni nodo KSN offre una panoramica dettagliata delle minacce affrontate dagli utenti, contribuendo a creare un corpo di threat Intelligence che rende Internet più sicuro per tutti. Un buon esempio di come possono essere potenti le panoramiche: KSN ha rilevato i moduli di attacco mirato altamente sofisticati di Equation molto tempo prima che venisse identificato come gruppo organizzato e coordinato per le minacce. Il dropper trojan di Equation, "EquationLaser" e il worm "Funny" sono stati rilevati e bloccati da KSN, rispettivamente, ad aprile 2012 e giugno 2013.

Ciò che rende tanto interessante il ruolo di KSN nel rilevamento dell'APT di Equation è il fatto che illustra perfettamente il ruolo che possono giocare privati e piccole aziende nella ricerca di minacce sofisticate.. Molti di questi utenti partecipano a KSN e abbiamo imparato molto dalla threat information da loro fornita; è sorprendente quanto gli utenti domestici o di piccole aziende rappresentino una fonte estremamente preziosa di threat intelligence per i clienti aziendali. Questo accade in parte perché tendono ad avere comportamenti online ad alto rischio, ma anche perché i cybercriminali spesso li usano come trampolino per lanciare attacchi contro le reti aziendali più sicure.

Diamo ora uno sguardo a come la protezione basata su cloud di KSN utilizzi questi dati per ottenere tassi di rilevamento migliori, ridurre i tempi di reazione, minimizzare i falsi positivi e supportare il whitelisting.

L'IMPORTANZA DEI TASSI DI RILEVAMENTO

Gli analisti di Kaspersky Lab rilevano ogni giorno 360.000 nuovi file malware; ogni mese vengono aggiunte 113.500 wildcard di phishing al nostro database anti-phishing.

Il cybercrimine è cresciuto, non solo in termini di volumi, ma anche in raffinatezza; mentre il 70% delle minacce che colpiscono le aziende ogni giorno sono note, il 30% sono sconosciute e avanzate e la tradizionale sicurezza basata su firma non è più all'altezza. La threat intelligence acquisita con il monitoraggio di esperti 24 ore su 24, 7 giorni su 7 delle minacce che affrontano respingono gli utenti rappresenta un componente chiave del sistema di difesa multilivello di Kaspersky Lab. Kaspersky Security Network (KSN) gioca un ruolo chiave nella creazione di questo panorama.

KSN elabora più di 600.000 richieste, trasportando 14 Gb di statiche globali in entrata al secondo. Questa intelligence costantemente aggiornata consente agli utenti KSN di usufruire di un aumento dei tassi di rilevamento dal 2,5 al 3,1%. Lo scorso anno più del 39% degli utenti di KL ha affrontato minacce, sia conosciute che sconosciute, che i componenti anti-virus standard non sarebbero stati in grado di rilevare, mentre KSN lo ha fatto. Il 20% delle minacce rilevate dalle tecnologie Kaspersky Lab viene rilevato utilizzando le statistiche raccolte da KSN.

Proviamo a pensare: nell'attuale ambiente delle minacce, anche una differenza dello 0,9% nei tassi di rilevamento tassi si può tradurre in centinaia di migliaia di malware passati attraverso la rete nel corso di un anno. E si tratta di questo di 1% di attacchi mirati che in genere è più dannoso per i sistemi aziendali, in quanto spesso non vengono rilevati per mesi o addirittura anni.

Questo frammento aggiuntivo di esperienza e protezione fornito da KSN può rappresentare la vera minaccia che la vostra azienda vuole evitare, specialmente quando si tratta di APT e malware più avanzati. L'analisi della "catena della criminalità informatica" mostra che gli utenti malintenzionati devono superare ogni punto della catena per raggiungere il loro obiettivo: una sola mitigazione distruggerebbe sia la catena che l'utente malintenzionato.[1]

[1] EM Hutchins, MJ Cloppert, RM Amin: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.

LA TEMPESTIVITÀ È TUTTO

Se è importante ridurre il numero di minacce che passano attraverso la rete, è altrettanto importante il tempo impiegato per il rilevamento e la risposta. Le velocità di rilevamento e blocco basate su cloud di KSN sono di gran lunga superiori rispetto a quanto offerto dagli aggiornamenti agli anti-malware tradizionali. I processi standard di rilascio e aggiornamento della firma possono impiegare ore e il margine di miglioramento è ridotto.

Gli aggiornamenti assistiti dal cloud, come quelli offerti da KSN, d'altra parte, consentono una condivisione della threat intelligence quasi in tempo reale per quanto riguarda minacce nuove ed emergenti, modelli di comportamenti sospetti, link dannosi o siti web pericolosi, tutto in 30-40 secondi.

Proviamo a pensare: quando si tratta di minacce avanzate e sofisticate, un ritardo nella risposta anche di poche ore può portare a gravi conseguenze.

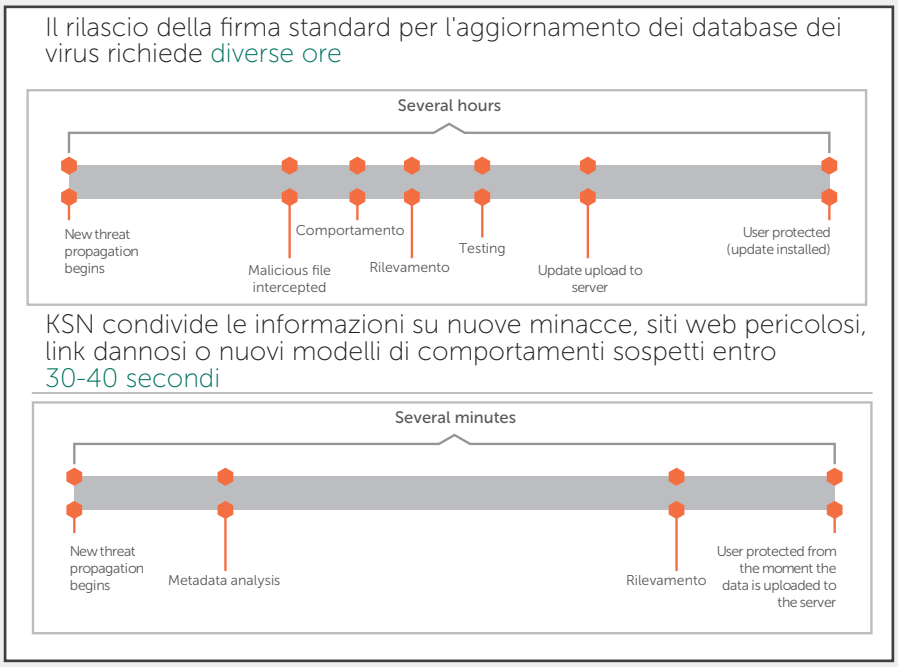


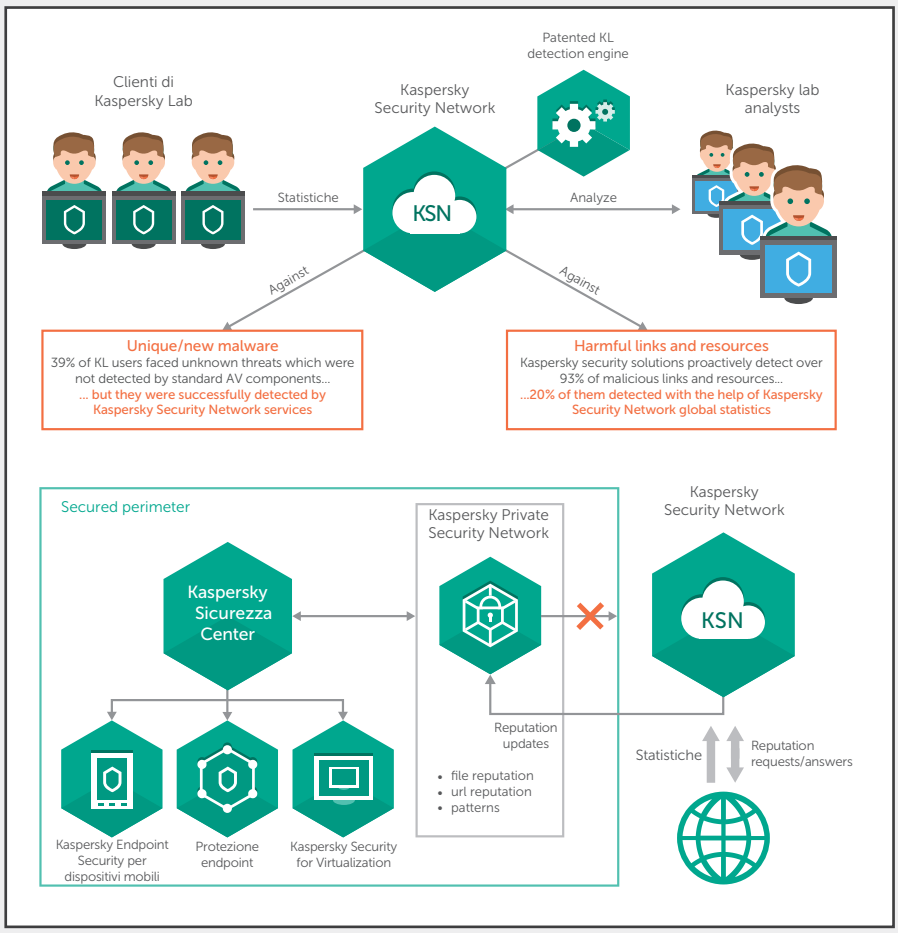
Figura 1: Riduzione dei tempi di reazione alla minaccia con Kaspersky Security Network: visione globale, proattiva e in tempo reale.

ELIMINARE I FALSI POSITIVI

In qualsiasi sistema che analizza grandi volumi di file, i falsi positivi possono diventare un problema irritante e spesso molto impegnativo in termini di tempo. La maggiore velocità e flessibilità della sicurezza assistita dal cloud riduce i tempi di aggiornamento, portando ad una sempre maggiore precisione e riducendo i falsi positivi.

Nessuna organizzazione desidera dedicare il proprio tempo alle attività costanti di compilazione, revisione e aggiornamento degli elenchi di applicazioni "sicure" e accettabili. E per quanto riguarda i driver delle stampanti, i software di rete e gli aggiornamenti essenziali? In che modo è possibile accertarsi che gli aggiornamenti essenziali non vengano erroneamente contrassegnati come pericolosi?
Ci pensa la whitelist dinamica di Kaspersky Lab. Prodotto da un Whitelist lab dedicato, in collaborazione con centinaia di partner internazionali, è fondamentale che un enorme database di software "puliti" venga continuamente aggiornato con informazioni su tipi di file, aggiornamenti, file di installazione e, cosa più importante, informazioni su di essi. Sul database di Kaspersky Lab sono presenti circa 1,5 miliardi di file a cui Kaspersky Security Network ha sempre accesso.
Un programma classificato come "pulito" oggi, può trasportare un codice dannoso domani e solo il monitoraggio e l'analisi costanti possono garantire informazioni affidabili sulla reputazione. Un'analisi indipendente condotta da West Coast Labs ha rilevato che il database basato su cloud di Kaspersky Lab contiene dati sul 94% di tutti i software puliti rilasciati a livello globale.
Nessun cloud di sicurezza è perfetto; i file e gli URL dannosi possono occasionalmente essere etichettati come attendibile/non attendibile. Inoltre, viene eseguita continuamente un'analisi delle prestazioni per migliorare la qualità.

INTRODUZIONE A KASPERSKY PRIVATE SECURITY NETWORK PER CONFORMITÀ, CRITERI DI SICUREZZA E REQUISITI DI AFFIDABILITÀ ESCLUSIVI



La prima immagine mostra come funziona Kaspersky Security Network. La seconda mostra come Kaspersky Private Security Network opera interamente all'interno dell'infrastruttura aziendale.

Ora che avete compreso i vantaggi e le funzionalità di KSN, diamo un'occhiata a come Kaspersky Private Security Network soddisfa le esigenze delle organizzazioni caratterizzate da rigorosi controlli dei dati.

La prima cosa da ricordare è che, mentre i dati sono sempre resi completamente anonimi da KSN, Kaspersky Private Security Network porta il livello di protezione un passo avanti portando il cloud in locale e garantendo così che l'organizzazione possa mantenere il controllo completo di tutti i dati, traendo allo stesso tempo vantaggio dalla threat intelligence raccolte da KSN.

KASPERSKY PRIVATE SECURITY NETWORK: VANTAGGI GLOBALI, FORNITI IN LOCALE

Kaspersky Private Security Network può essere installata all'interno dei data center dell'organizzazione e gli specialisti interni dell'IT/sicurezza possono averne il controllo completo. Allo stesso tempo, l'organizzazione ha a disposizione tutti i vantaggi per la sicurezza: analisi delle minacce in tempo reale, analisi della reputazione, rilevamento proattivo delle minacce e whitelisting dinamico.

KPSN è particolarmente adatto alle aziende che devono rispettare in maniera rigorosa la conformità o standard governativi o industriali. Esiste anche un'opzione di implementazione di tipo "air-gap" disponibile per i segmenti di rete in cui non si desidera la connessione Internet.

Inoltre, mentre la maggior parte dei fornitori di protezione assistita dal cloud offre dei "proxy cache" che consentono di ridurre il numero di volte in cui il sistema deve contattare il cloud per i dati di reputazione, Kaspersky Lab è l'unica che ha la possibilità di implementare il cloud interamente in locale, all'interno dei data center dell'organizzazione e senza nessuna transazione in uscita con server di terze parti. Questa funzionalità è fondamentale in alcune configurazioni industriali e governative.

Per una maggiore sicurezza, l'implementazione KPSN conserva database di firme locali. Quando alcune soluzioni migrano completamente questa capacità al cloud, durante la migrazione il cliente resta esposto agli attacchi. Con KPSN questo non avviene; durante la fase di implementazione i database locali di Kaspersky Lab (che possono essere aggiornati manualmente) continuano a fornire una protezione ottimale, eliminando eventuali falle nel sistema di sicurezza.

Una volta attivo e in esecuzione, KPSN può diventare una fonte di threat intelligence e informazioni esclusive per altre eventuali soluzioni in esecuzione: centro operativo di sicurezza, SIEM, gestione dei rischi, GRV, processi forensi e di correzione... tutto può essere integrato con i feed di dati, offrendo una panoramica della sicurezza e della capacità di risposta alle minacce dell'organizzazione.


Twitter.com/
KasperskyLabIT


Facebook.com/
Kasperskylabitalia


Youtube.com/
Kasperskyitalia

Kaspersky Lab, Mosca, Russia
www.kaspersky.it

Tutto sulla sicurezza in Internet:
www.securelist.com

Trovate il partner più vicino:
www.kaspersky.it/buyoffline

KASPERSKY lab