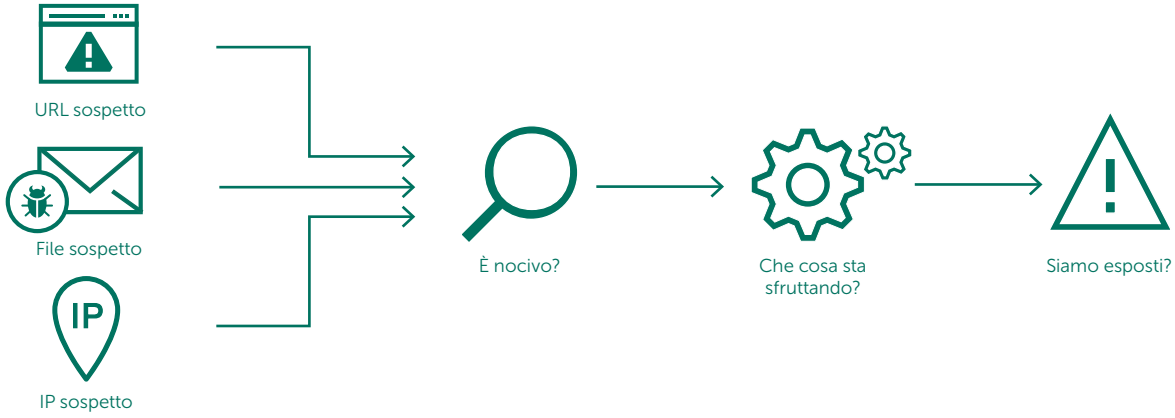

# CHIUDERE IL CERCHIO DELLE PROTEZIONI PER LA RETE

KASPERSKY lab

Oggi, il cybercrime non conosce confini e le capacità tecniche mostrano un rapido miglioramento: vediamo attacchi diventare di volta in volta più sofisticati e cybercriminali utilizzare risorse del Dark Web per minacciare i propri obiettivi. Le cyberminacce registrano una costante crescita in termini di frequenza, complessità e tecniche di offuscamento, con un numero sempre maggiore di tentativi di compromissione delle soluzioni di protezione. I cybercriminali, nelle loro campagne, utilizzano complessi attacchi a catena, tattiche, tecniche e procedure personalizzate (TTP) mirati a bloccare i processi aziendali, a rubare le risorse o a danneggiare i clienti.

L'accesso a Kaspersky Threat Lookup offre intelligence affidabile e immediata su cyberminacce, oggetti legittimi, interconnessioni tra di essi e indicatori, ed è completa del contesto di applicabilità, al fine di consentire ad aziende e clienti di prendere coscienza dei rischi e delle implicazioni associati. Oggi è possibile mitigare e rispondere alle minacce in modo più efficace, difendendosi dagli attacchi ancor prima che vengano sferrati.
Kaspersky Threat Lookup fornisce tutte le conoscenze acquisite da Kaspersky Lab sulle cyberminacce e sulle relazioni tra di esse, riunite in un unico e potente servizio Web. L'obiettivo è fornire ai team per la sicurezza delle aziende la maggior quantità possibile di dati, per prevenire gli attacchi informatici prima che compromettano l'organizzazione. La piattaforma recupera la threat intelligence più dettagliata e recente su URL, domini, indirizzi IP, hash dei file, nomi delle minacce, dati statistici/analisi comportamentale, dati WHOIS/DNS e così via. Il risultato è la visibilità a livello globale delle minacce nuove ed emergenti, al fine di aiutare i clienti a mettere in sicurezza la propria organizzazione e migliorare la risposta agli incidenti.




## Funzionalità:

- **Intelligence affidabile:** una caratteristica chiave di Kaspersky Threat Lookup è l'affidabilità dei dati della threat intelligence, completati dal contesto di applicabilità. I prodotti Kaspersky Lab sono leader nel settore secondo i risultati dei test condotti sulle soluzioni anti-malware1, grazie a un'impareggiabile intelligence di sicurezza e a tassi di rilevamento più elevati, che garantisco una quantità di falsi positivi quasi pari a zero.
- **Copertura elevata e in tempo reale:** la threat intelligence viene automaticamente generata in tempo reale, sulla base delle scoperte a livello mondiale (grazie a Kaspersky Security Network, che garantisce accesso a una percentuale notevole di tutto il traffico Internet e a tutti i tipi di dati, arrivando a coprire dieci milioni di utenti finali in oltre 213 paesi) che offrono copertura e accuratezza elevate.
- **Threat Hunting:** proattività nella prevenzione, nel rilevamento e nella risposta agli incidenti, al fine di ridurre al minimo l'impatto e la frequenza. Monitoraggio e allontanamento aggressivo dei cybercriminali nel minor tempo possibile. Quanto prima la minaccia viene rilevata, tanto minore sarà il danno causato. Quanto più rapidamente hanno luogo le correzioni, tanto prima le attività di rete possono tornare al normale funzionamento.
- **Grande varietà di dati:** la threat intelligence offerta da Kaspersky Threat Lookup copre una gamma enorme di tipi differenti di dati, tra cui informazioni relative ad hash, URL, IP, whois, pDNS, GeoIP, attributi dei file, dati statistici e analisi comportamentale, catene di download, marcature temporali e tanto altro. Con il supporto di questi dati, è possibile sondare il variegato panorama delle minacce alla sicurezza che le aziende si trovano ad affrontare.
- **Disponibilità continua:** la threat intelligence viene generata e monitorata da un'infrastruttura ad elevata tolleranza di errore, che garantisce disponibilità continua dei dati e prestazioni costanti.
- **Analisi continua da parte degli esperti di sicurezza:** centinaia di esperti, tra cui analisti della sicurezza provenienti da tutto il mondo, esperti di sicurezza di fama mondiale del team GReAT e di team di Ricerca e Sviluppo all'avanguardia, contribuiscono alla creazione di una threat intelligence di valore, basata su situazioni reali.

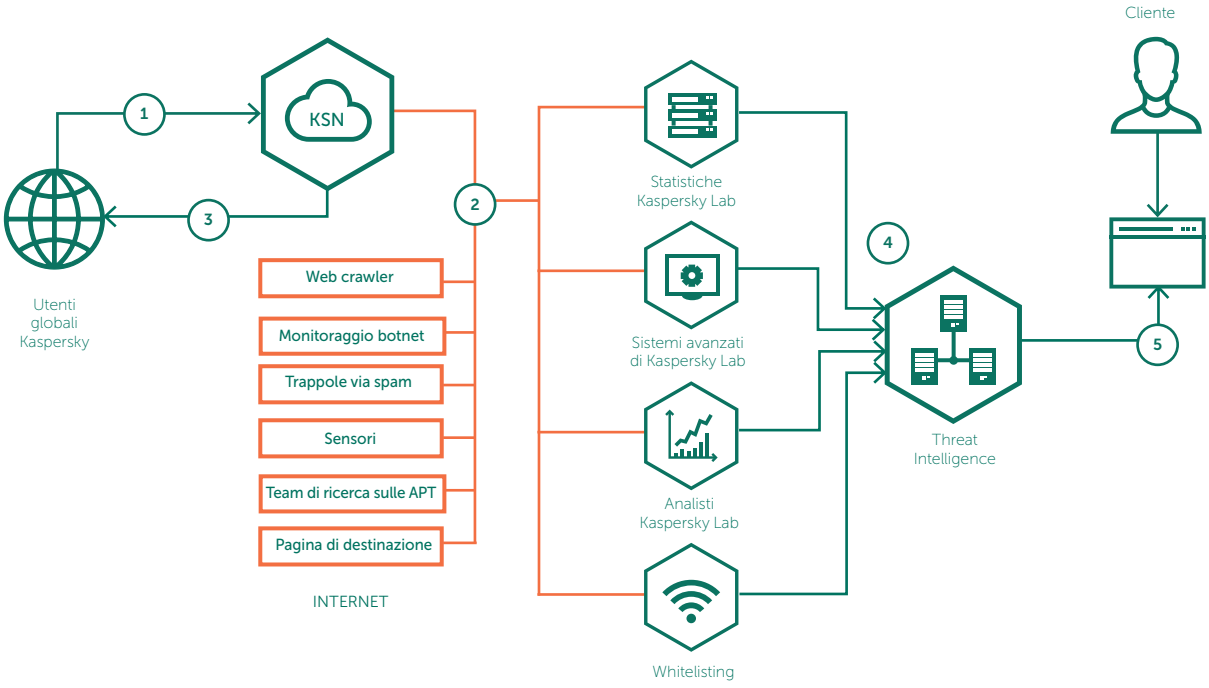
- **Analisi della sandbox:**[2] consente di rilevare le minacce sconosciute eseguendo oggetti sospetti in un ambiente sicuro e analizzando il comportamento completo della minaccia e degli artefatti tramite report intuitivi.
- **Ampia gamma di formati di esportazione:** è possibile esportare gli indicatori di compromissione (IOC) o il contesto di applicabilità nei formati di condivisione leggibili dai computer maggiormente utilizzati e organizzati, come STIX, OpenIOC, JSON, Yara, Snort o addirittura CSV, per usufruire di tutti i vantaggi della threat intelligence, per automatizzare il flusso di lavoro operativo o per effettuare l'integrazione con controlli di sicurezza quali SIEM.
- **Interfaccia Web o API RESTful di facile utilizzo:** consente di utilizzare il servizio in modalità manuale tramite un'interfaccia Web (via browser Web) o di accedervi tramite una semplice API RESTful, a seconda delle preferenze.

## Vantaggi chiave:

- **Miglioramento e accelerazione della risposta agli incidenti e delle capacità di analisi forense,** fornendo ai team di sicurezza/SOC aziendali informazioni importanti sulle minacce, nonché un esame approfondito di ciò che sottende gli attacchi mirati. Efficacia ed efficienza migliorate per la diagnosi e l'analisi degli incidenti di sicurezza su host e rete, con assegnazione della priorità ai segnali di minacce sconosciute derivanti da sistemi interni, riduzione al minimo dei tempi di risposta agli incidenti e interruzione degli attacchi a catena prima che vengano compromessi sistemi e dati critici.
- **Conduzione di ricerche approfondite sugli indicatori di minaccia,** quali indirizzi IP, URL, domini o hash di file, con contesto della minaccia ad elevata validità, che consente di assegnare le priorità agli attacchi, migliorare lo staff e le decisioni in merito all'allocazione delle risorse, nonché di concentrarsi sulla mitigazione della minaccia, che rappresenta il rischio maggiore per l'azienda.
- **Mitigazione degli attacchi.** Miglioramento dell'infrastruttura di sicurezza aziendale con threat intelligence tattica e strategica, che adatta le strategie di difesa per rispondere alle minacce specifiche affrontate dall'organizzazione.

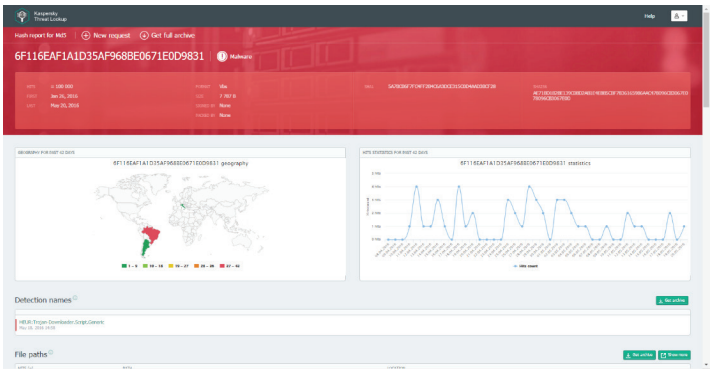
## Fonti di Threat Intelligence:

La threat intelligence è un aggregato derivante dalla fusione di fonti eterogenee e ad elevata affidabilità, tra cui Kaspersky Security Network (KSN), Web crawler, servizio di monitoraggio delle botnet (monitoraggio 24 ore al giorno, 7 giorni la settimana, 365 giorni all'anno dei botnet, degli obiettivi e delle attività a essi relativi), trappole via spam, team di ricerca, partner e altri dati storici sugli oggetti dannosi, raccolti da Kaspersky Lab in oltre 2 decenni. In tempo reale, dunque, tutti i dati aggregati vengono accuratamente ispezionati e perfezionati tramite diverse tecniche di pre-elaborazione, quali criteri statistici, sistemi avanzati di Kaspersky Lab (sandbox, motori di euristica, strumenti per la somiglianza, profiling comportamentale e così via), convalida da parte degli analisti e verifica del whitelisting.



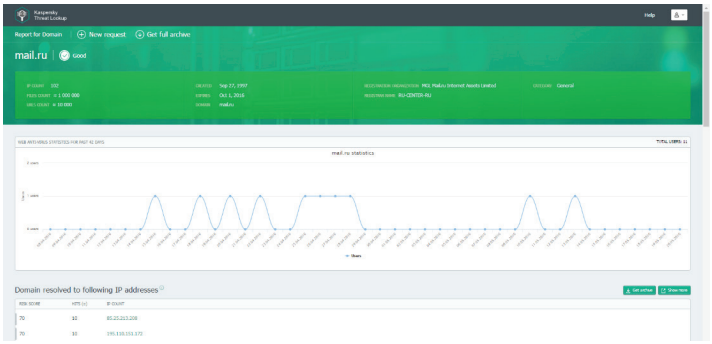

Kaspersky Threat Intelligence comprende dati, analizzati a fondo, sugli indicatori della minaccia, derivanti da situazioni reali, in tempo reale.

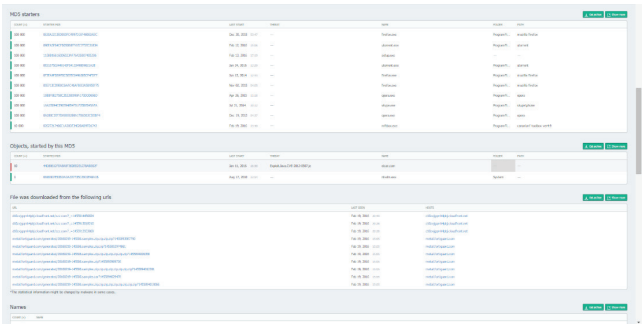
[1] http://www.kaspersky.com/top3
[2] Il lancio della funzionalità è previsto per il 1° trimestre 2017.



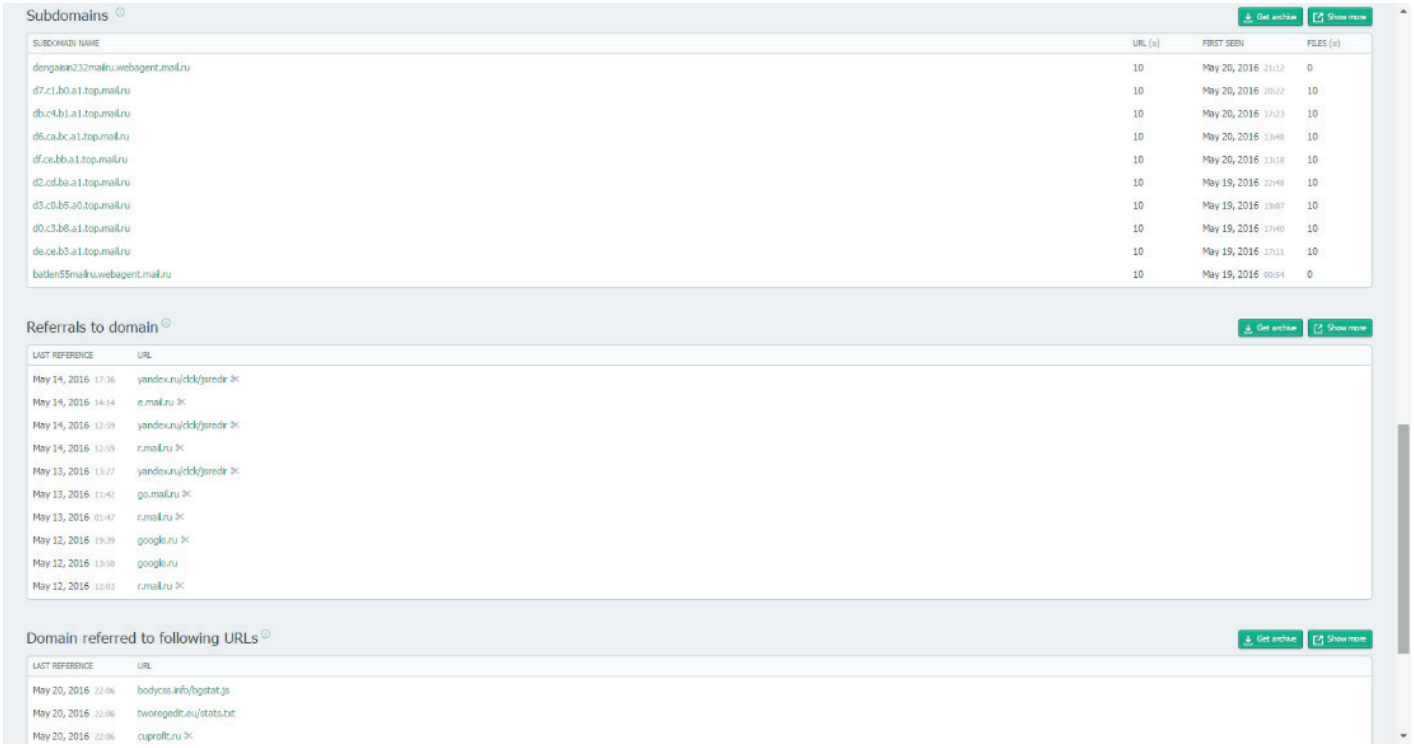

## Adesso è possibile:

- Esaminare gli indicatori di minaccia tramite un'interfaccia basata sul Web o l'API RESTful.
- Comprendere il motivo per cui un oggetto deve essere considerato pericoloso.
- Controllare se l'oggetto rilevato è singolo o diffuso.
- Analizzare dettagli avanzati tra cui certificati, nomi comunemente utilizzati, percorsi di file o URL correlati per scoprire nuovi oggetti sospetti. Questi sono solo alcuni esempi: la ricca e ininterrotta fonte di dati di intelligence pertinenti e granulari può essere usata in tanti modi diversi.



Conoscere nemici e amici. Riconoscere i file, gli URL e gli indirizzi IP di cui sia stata comprovata la non pericolosità, aumentando la velocità di indagine. Quando ogni secondo può essere cruciale, non sprecare tempo nell'analisi degli oggetti affidabili è di vitale importanza.




La nostra missione è salvare il mondo da tutti i tipi di cyberminacce. Proprio per questo, e per consentire a tutti di navigare in Internet in tutta sicurezza, è essenziale condividere e accedere in tempo reale alla threat intelligence. Un accesso tempestivo alle informazioni è fondamentale per garantire una protezione efficace di dati e reti aziendali. Ora, Kaspersky Threat Lookup semplifica e rende più efficiente l'accesso a questa intelligence. Come mai prima.

KASPERSKY lab
THE POWER
OF PROTECTION