



Imparate a difendervi dai vostri nemici: scoprite il vero panorama delle minacce per la vostra organizzazione

Panorama delle minacce informatiche su Kaspersky Threat Intelligence Portal

kaspersky bring on
the future



Kaspersky Threat Intelligence Portal

Panorama delle minacce per l'organizzazione su Kaspersky Threat Intelligence Portal

Il panorama delle minacce globali è in continua evoluzione: ogni giorno emergono nuovi metodi di attacco e quelli già noti diventano sempre più sofisticati. Oggi è sempre più importante che i team per la sicurezza delle informazioni siano in grado di stabilire in modo efficace le priorità delle minacce che devono essere affrontate rapidamente. Ma come concentrarsi sulle minacce più rilevanti per la propria azienda, il proprio settore e la propria area geografica?



Portale Kaspersky Threat Intelligence

Gli utenti hanno un'opportunità unica di valutare il panorama delle minacce nella sezione **Panorama delle minacce informatiche**, che è stata specificamente progettata per fornire informazioni sugli autori degli attacchi che prendono di mira un settore e un'area geografica specifica. La sezione offre un contesto completo e aggiornato sulle minacce associate ai potenziali avversari, alle loro tattiche, tecniche e procedure (TTP).

Panorama delle minacce informatiche fornisce informazioni sulle minacce associate a:



area geografica



settore



tipi di minaccia



threat actor



tecniche, tattiche e procedure (TTP)



software dannoso utilizzato

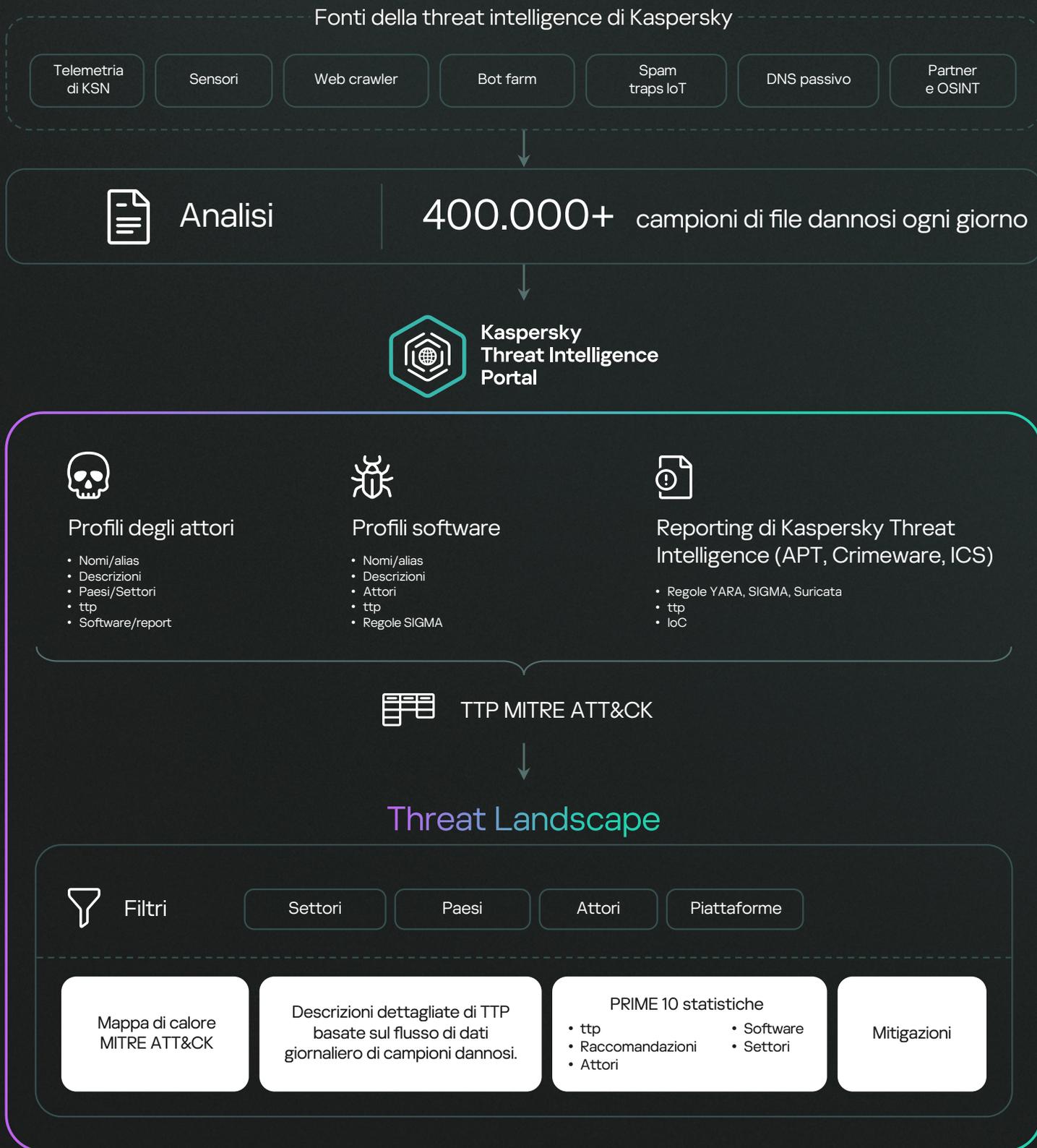


indicatori di compromissione (IoC)

I dati di intelligence sulle minacce vengono raccolti **in tempo reale utilizzando una serie di sistemi avanzati** di cui Kaspersky si serve da oltre 25 anni per combattere la criminalità informatica: Kaspersky Security Network, che riceve dati anonimi da milioni di utenti in tutto il mondo, elaborando automaticamente milioni di file al giorno, Web crawler, bot farm, spam traps, honeypot, sensori, DNS passivo, fonti e partner dell'Open e del Dark Web. Noi stessi abbiamo utilizzato questi dati nell'ultimo quarto di secolo, ottenendo i punteggi più alti nei test indipendenti e nelle recensioni esterne. I dati ottenuti vengono attentamente analizzati dai team Kaspersky, dedicati alla ricerca delle minacce. Dati che vengono inoltre elaborati da moderni sistemi automatizzati come sandbox, motori euristici e strumenti di similarità, trasformandoli in informazioni verificate e aggiornate.

Per saperne di più

Come funziona

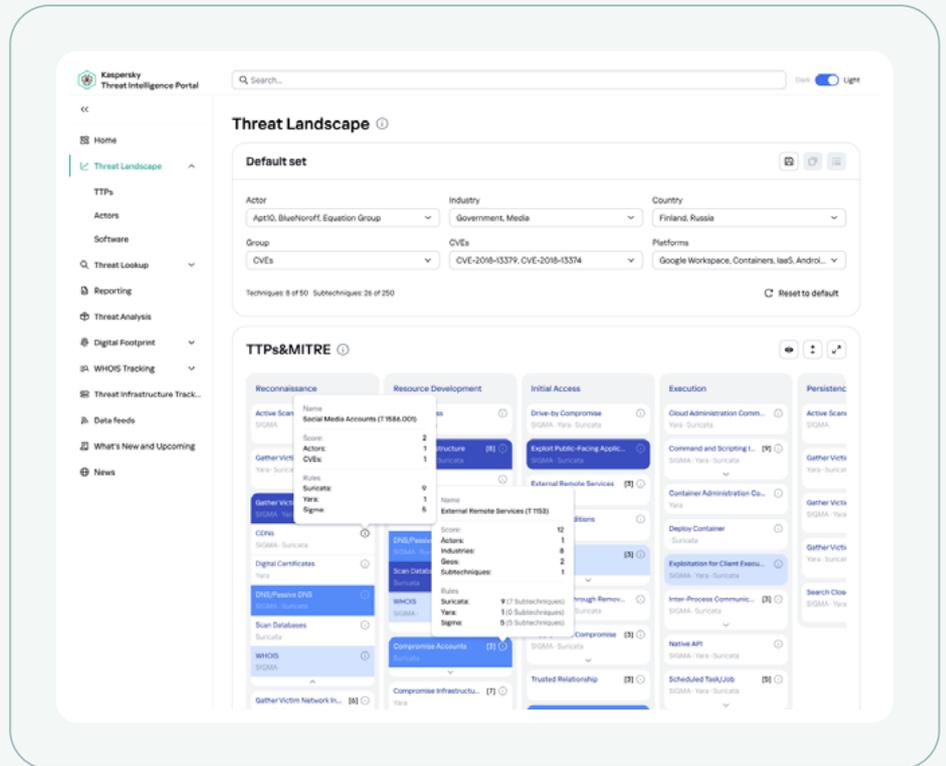


Elaboriamo **centinaia di migliaia di campioni di file dannosi ogni giorno**, estraendo i dati di geolocalizzazione e di settore. I sistemi interni di Kaspersky estraggono quindi le TTP associate e attribuiscono i file a gruppi di criminali informatici e malware già noti. La sezione Panorama delle minacce informatiche si basa anche su un flusso di dati di incidenti reali provenienti da tutto il mondo, che riceviamo dai nostri team di ricerca formati da esperti.

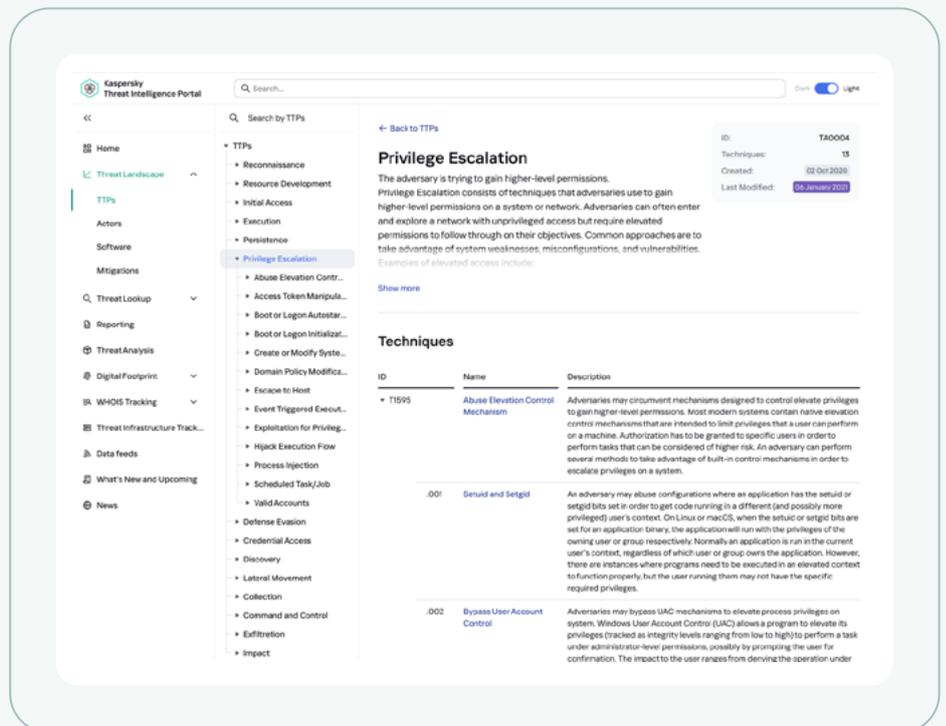
Dopo aver applicato i filtri, gli utenti di Kaspersky Threat Intelligence Portal sono in grado di creare il proprio panorama delle minacce, **in linea con il framework MITRE ATT&CK**, ottenendo le informazioni più aggiornate sui potenziali avversari: tecniche, tattiche e procedure più probabilmente utilizzate per gli attacchi, descrizioni dettagliate degli attori, del malware e delle TTP utilizzate, report con una descrizione dettagliata degli attacchi e, infine, le mitigazioni, ovvero raccomandazioni specifiche che consentono di evitare che una tecnica venga messa in atto con successo.

Caratteristiche principali

Mapa di calore MITRE ATT&CK per elaborare un **panorama delle minacce unico per l'organizzazione** in tempo reale. Applicando i filtri, l'utente ha accesso ai dati più recenti, inclusi gli aggiornamenti delle ultime 24 ore, ottenuti dai nostri sistemi e dai nostri esperti attraverso una ricerca continua. L'utente, avrà la possibilità di salvare i filtri per una successiva analisi.



Informazioni in tempo reale sulle **tecniche, le tattiche e le procedure** degli autori degli attacchi, basate sui sistemi avanzati di Kaspersky.



La sezione delle mitigazioni fornisce **descrizioni dettagliate** delle **misure di protezione** e di prevenzione che le organizzazioni devono adottare per evitare falle nella sicurezza.

The screenshot displays the 'Application Developer Guidance' page in the Kaspersky Threat Intelligence Portal. The page is titled 'Application Developer Guidance' and includes a sub-header 'Techniques Addressed by Mitigation'. Below this, there is a table with columns for ID, Name, and Description. The table lists various techniques such as 'Exploitation for Credentials', 'Hide Artifacts: Resource', 'Hijack Execution Flow', 'DLL Side Loading', 'User Process Communi...', 'Pilot File Modification', 'Search Open Websites', 'Domain Policy Modifi...', 'Escape to Host', 'Event Triggered Execu...', 'Exploitation for Privileg...', 'Hijack Execution Flow', and 'Process Injection'. Each entry includes a brief description of the technique and its potential impact. The page also features a 'References' section with several links to external sources.

Accesso al **repository più vasto** del settore di **profili di attori** e di **malware** con descrizioni dettagliate compilate dagli esperti Kaspersky.

The screenshot displays the profile of the APT10 actor in the Kaspersky Threat Intelligence Portal. The profile includes a header with the actor's name 'Apt10' and a sub-header 'Description'. Below this, there is a text block providing a detailed description of the actor, including their background and activities. The profile also features a world map showing the actor's activity across various regions, with a legend indicating the actor's primary locations: Athens, Madagascar, Andhra, and Bangladesh. The page includes a 'Show more' link and a 'References' section with several links to external sources.

Accesso alle regole Sigma/Yara/Suricata relative alle tecniche, alle tattiche e alle procedure MITRE ATT&CK per rilevare le minacce rilevanti per l'organizzazione.

The screenshot displays the Kaspersky Threat Intelligence Portal. The left sidebar contains navigation options like Home, Threat Landscape, TTPs, and various threat intelligence sources. The main content area is divided into two sections: 'Tactics Techniques and Procedures' and 'Reports'. The TTPs section shows a table with columns for Tactic, Technique, Severity, and Details. The Reports section shows a list of reports with columns for Date, Title, Origin, Report ID, Report, and Tags.

PRIME 10 statistiche su settori, attori, TTP, vulnerabilità e software.

The infographic presents six categories of top 10 statistics:

- Attacks by Industry:**
 - 1 IT & Telecommunications (22.03%)
 - 2 Business Services (20.12%)
 - 3 Education (18.03%)
 - 4 Energy & Utilities (15.64%)
 - 5 Government (12.56%)
 - 6 Finance (10.85%)
 - 7 Healthcare (8.56%)
 - 8 Telecommunications (7.63%)
 - 9 Retail & Wholesale (5.36%)
 - 10 Hospitality (4.33%)
- Top Actors:**
 - 1 BlueHornoff (33.03%)
 - 2 Sofacy (26.12%)
 - 3 Finix (20.05%)
 - 4 UNC4542 (18.66%)
 - 5 APT10 (15.56%)
 - 6 Equation Group (10.85%)
 - 7 Carbanem (8.56%)
 - 8 Senuwurm (7.63%)
 - 9 Evil Corp (5.36%)
 - 10 Fancy Bear (4.33%)
- Top Utilities:**
 - 1 Cisco Umbrella (18.21%)
 - 2 dnSpy (15.65%)
 - 3 Echosec (3.31%)
 - 4 GreyNoise (2.4%)
 - 5 Insights External Threat Protection (2.39%)
 - 6 Lumina by Cognyster (2.02%)
 - 7 Recorded Future (1.92%)
 - 8 Threat Intelligence APIs (1.83%)
 - 9 ThreatFusion (1.5%)
 - 10 Zorlix (1.0%)
- Top Techniques:**
 - 1 Data Encrypted for Impact (18.21%)
 - 2 Inhibit System Recovery (15.65%)
 - 3 Obfuscated Files or Information (3.31%)
 - 4 Windows Management Instrumentation (2.4%)
 - 5 Manpowering (2.39%)
 - 6 Command and Scripting Interpreter (2.02%)
 - 7 Ingaif Defenses (1.92%)
 - 8 Modify Registry (1.83%)
 - 9 User Execution (1.5%)
 - 10 Process Injection (1.0%)
- Top Tactics:**
 - 1 Resource Development (23.21%)
 - 2 Privilege Escalation (5.65%)
 - 3 Defense Evasion (3.31%)
 - 4 Credential Access (2.4%)
 - 5 Lateral Movement (2.39%)
 - 6 Command and Control (2.02%)
 - 7 Eutfration (1.92%)
 - 8 Impact (1.83%)
 - 9 Collection (1.5%)
 - 10 Discovery (1.0%)
- Top Vulnerabilities:**
 - 1 Broken Access Control (18.21%)
 - 2 Cryptographic Failures (5.65%)
 - 3 Injection (3.31%)
 - 4 Insecure Design (2.4%)
 - 5 Vulnerable and Outdated Components (2.39%)
 - 6 Identification and Authentication Failures (2.02%)
 - 7 Software and Data Integrity Failures (1.92%)
 - 8 Security Logging and Monitoring Failures (1.83%)
 - 9 Server Side Request Forgery (1.5%)
 - 10 Security Misconfiguration (1.0%)



Il mondo in continua evoluzione delle cyberminacce contiene oggi una grande quantità di **dati di threat intelligence** disponibili attraverso una varietà di prodotti e servizi. Comprendendo il panorama di minacce, le organizzazioni sono in grado di adottare misure strategicamente ragionevoli per difendersi in modo proattivo da attacchi specifici.

Vantaggi dell'utilizzo

Approccio proattivo alla difesa

Imparate a conoscere i vettori di attacco più probabili per l'organizzazione al fine di creare una strategia di difesa efficace

Monitoraggio della superficie di attacco

Identificate le falle nella sicurezza prima che gli autori degli attacchi le sfruttino

Puntare sulle minacce rilevanti

Possibilità di concentrarsi sulle minacce che più probabilmente interesseranno la propria azienda, il proprio settore e la propria area geografica

Pianificazione strategica

Utilizzate le informazioni sul panorama delle minacce per la pianificazione degli investimenti e lo sviluppo di strumenti e metodi di protezione

Maggiore efficienza dei reparti di sicurezza delle informazioni

Aumentate l'efficienza del personale e riducetene i costi grazie all'accesso alle informazioni sulle minacce rilevanti e sulle tendenze globali.

Consapevolezza delle minacce

Consapevolezza delle minacce più recenti e delle tendenze globali per una difesa efficace



Se conosci il nemico e conosci te stesso, non dovrai temere l'esito di cento battaglie. Se conosci te stesso, ma non il tuo avversario, per ogni vittoria subirai una sconfitta. Se non conosci te stesso né il tuo rivale, perderai in ogni battaglia

Sun Tzu

da L'arte della guerra

Kaspersky Threat Intelligence

Kaspersky Threat Intelligence consente di accedere a una serie di informazioni raccolte dai nostri analisti e ricercatori di livello mondiale. Questi dati aiuteranno qualsiasi organizzazione a **contrastare efficacemente le odierne minacce informatiche**.

La nostra azienda dispone di una profonda conoscenza, di una vasta esperienza nella ricerca sulle minacce informatiche e di una visione unica di tutti gli aspetti della sicurezza informatica. Questo ha reso Kaspersky un partner affidabile delle forze dell'ordine e delle organizzazioni governative di tutto il mondo, tra cui l'Interpol e diverse unità CERT. Kaspersky Threat Intelligence fornisce informazioni aggiornate sulle minacce tattiche, operative e strategiche.



Kaspersky Threat Intelligence

Per saperne
di più

www.kaspersky.it

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

#kaspersky
#bringonthefuture