KASPERSKY lab

Protezione avanzata e threat intelligence per mitigare il rischio di attacchi mirati

Soluzione Kaspersky Threat Management and Defense

www.kaspersky.it
#truecybersecurity

Il crescente rischio di minacce avanzate e attacchi mirati

Il 15% delle aziende ha affrontato un attacco mirato, con oltre il 53% di casi in cui è stata registrata una conseguente perdita di dati sensibili*.

*Report sui rischi globali per la sicurezza IT 2015 di Kaspersky

Ogni azienda di dimensioni tali da occupare un posto importante sul mercato rappresenta un potenziale obiettivo. Ciò non vuol dire che le realtà più piccole siano immuni da questi attacchi: in molti casi, i criminali considerano queste aziende come punti di accesso, semplici da violare, attraverso i quali raggiungere l'obiettivo più grande. Ma quando si tratta di leader di mercato, le probabilità di diventare una vittima di un attacco del genere aumentano sostanzialmente. Non si tratta di "se", ma di "quando"...

Panorama delle minacce alle imprese

Gli attacchi mirati e le minacce avanzate, incluse le Advanced Persistent Threat (APT), rappresentano tra i rischi più pericolosi per i sistemi delle imprese. Tuttavia, mentre le minacce e le tecniche che utilizzano i cybercriminali sono in continua evoluzione, troppe organizzazioni fanno affidamento su tecnologie di sicurezza e mentalità obsolete per proteggersi contro le attuali e future minacce.

Le minacce avanzate mirate possono passare inosservate per settimane, mesi o addirittura anni, mentre i loro attori, lentamente e silenziosamente, raccolgono informazioni e lavorano in maniera incrementale per sfruttare le specifiche vulnerabilità dei sistemi sotto attacco. A differenza del normale malware, le minacce avanzate e mirate vengono controllate e gestite dai criminali in modo attivo. L'obiettivo non si limita alla distribuzione del malware, bensì è quello di persistere all'interno del perimetro aziendale. Questi attacchi sono il risultato della paziente, spesso scrupolosa, ricerca da parte di attori che sono consapevoli di giocare una lenta partita per perseguire il proprio fine.

Perdita media derivante da un singolo attacco mirato:

Chi sta conducendo l'attacco?

Cybercriminali: vendono i dati al miglior offerente o semplicemente rubano denaro. Generalmente, sviluppano da soli i propri strumenti informatici o li acquistano sul Dark Web.

Aziende della concorrenza: cercano dati riservati o intendono addirittura effettuare un sabotaggio. Solitamente, "acquistano" i servizi dei mercenari informatici.

Mercenari informatici: esperti in spionaggio informatico, sviluppano da soli gli strumenti che utilizzano e vendono i propri "servizi" al miglior offerente.

Hacktivist: sostengono di lavorare per il "bene comune", sono creativi, utilizzano kit di strumenti complessi e rappresentano un problema serio per qualsiasi organizzazione che attiri la loro attenzione.

Agenzie governative: sebbene tendano a negarlo, è comunemente risaputo che i governi monitorino, su base regolare, individui, gruppi e aziende. Gli strumenti utilizzati da queste agenzie possono essere estremamente sofisticati, costosi e difficili da rilevare.

Fattori interni ed esterni che conducono alla violazione

I fattori chiave che contribuiscono al successo dello sviluppo di attacchi mirati su infrastrutture IT includono:

- Hidden e Shadow IT
- Connettività non controllata dei dispositivi IoT
- Dipendenza critica dalla digitalizzazione
- Mancanza di capacità di prevenzione e una visione più che ottimista sull'attuale sicurezza del perimetro
- Scarsa consapevolezza da parte dei dipendenti sui rischi per la sicurezza delle informazioni
- Mancanza di visibilità sull'ambiente IT e in particolare sul routing di rete
- Software e sistemi operativi obsoleti e di gestione di proprietà
- Mancanza di preparazione del team di cybersecurity per quanto riguarda la ricerca di malware, analisi forensi, incident response e threat intelligence

Qual è il rischio?

Rischi per tutte le organizzazioni:

- Transazioni non autorizzate
- Furto o corruzione di dati critici
- Processo Stealth di manipolazione
- Indebolimento da parte della concorrenza
- Ricatto, estorsione
- Furto d'identità

Rischi dei settori chiave dell'industria:

Servizi finanziari

- Transazioni non autorizzate
- Attacchi ad ATM con furto fisico di denaro
- Furto d'identità

Amministrazioni

- Manipolazione dei dati
- Spionaggio
- Disponibilità limitata dei servizi online
- Furto d'identità
- Atti di Hacktivism

Produzione e alta tecnologia

- Spionaggio (know how)
- Processi di tecnologia critica compromessi

Telecomunicazioni

- Attacco a clienti aziendali utilizzando le infrastrutture delle telecomunicazioni
- Manipolazione del server di posta elettronica per scopi di social engineering
- Controllo di fatturazione
- Manipolazione delle risorse Web per scopi di phishing
- Utilizzo di infrastrutture compromesse (dispositivi/IoT) per attacchi DDoS

Energia e Servizi

- Manipolazione con dati di calcolo
- Attacchi su reti tecnologiche con danni fisici

Mass media

- Hacktivism
- Sito web compromesso (defacing, phishing) e diffusione di attacchi di massa

Healthcare

- Furto di informazioni del paziente
- Attacchi ad apparecchiatura di telemedicina

Attacchi mirati: cybercrimine come professione aziendale

Cybercriminali e hacker di grande esperienza supervisionano la maggior parte degli attacchi mirati. Essi sanno come adattare ogni fase dell'attacco per eludere le difese tradizionali del passato, sfruttare le debolezze e massimizzare la quantità dei valori rubati, tra cui denaro dati riservati e altro ancora.

I vecchi criminali nerd della sicurezza si sono trasformati in professionisti per i quali il cybercrimine rappresenta un business. La loro unica motivazione nel mirare e attaccare qualsiasi impresa è il profitto ottimale, calcolato ancor prima di lanciare l'attacco, sulla base dei relativi costi e dei potenziali profitti. L'obiettivo è naturalmente quello di attaccare al minor costo possibile, con il massimo dei risultati finanziari.

La maggior parte dei attacchi mirati utilizza una combinazione di social engineering e un set di strumenti personalizzati. Il costo del lancio di un efficace attacco mirato è diminuito significativamente, con un corrispondente aumento del numero totale di attacchi a livello globale.

Che cosa è a rischio quando un'organizzazione cade vittima di un attacco mirato?

Danno diretto	Spesa reattiva
Correzione + Opportunità perse + Downtime	Sistemi + Personale + Formazione
	Per prevenire ulteriori violazioni

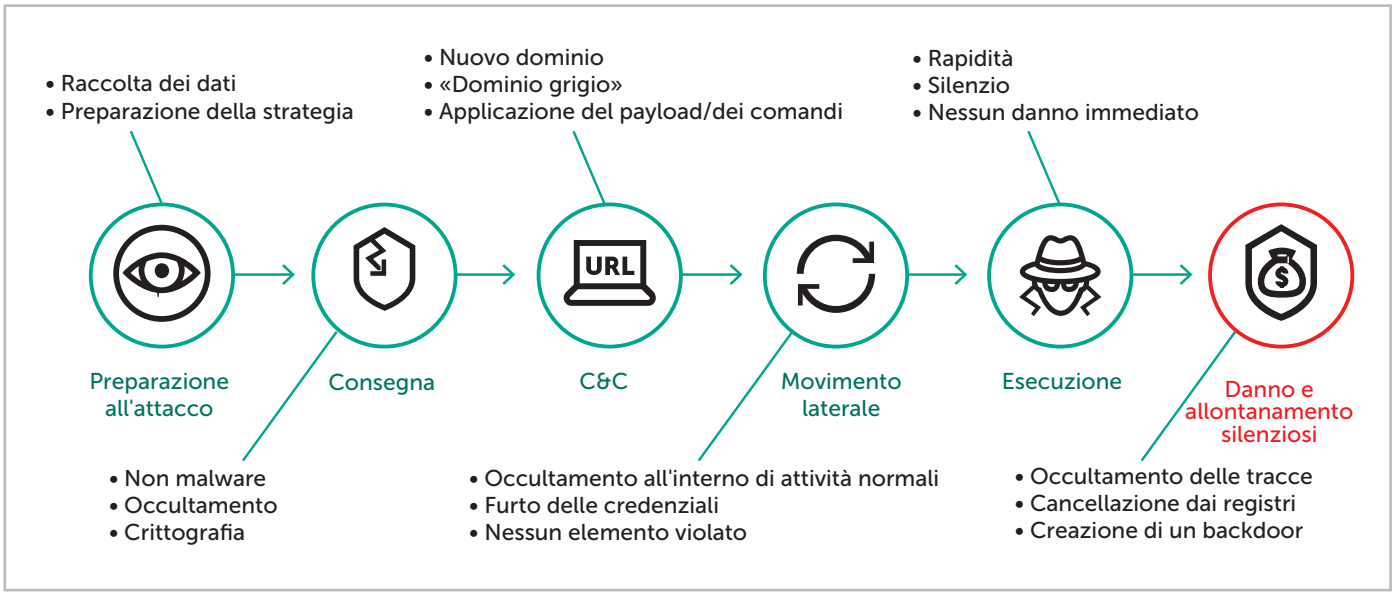
Direzione delle perdite finanziarie. Gli autori degli attacchi potrebbero tentare di commettere frodi informatiche, rubando le credenziali bancarie al fine di accedere a conti aziendali e di condurre transazioni fraudolente.

Interruzione dei principali processi aziendali. Alcuni attacchi, come meri prodotti secondari, potrebbero compromettere o rallentare processi aziendali critici, altri tipi di attacchi potrebbero invece puntare meticolosamente a sabotarli. Anche se un attacco è scoperto, c'è probabilmente un ulteriore periodo di interruzione durante il quale l'azienda conduce le indagini e ripristina le operazioni, nelle quali ulteriori opportunità aziendali potrebbero essere perse.

Costi di correzione. In seguito a un attacco, è possibile che si debbano affrontare spese considerevoli non messe a preventivo. I sistemi e i processi di ripristino potrebbero implicare spese di capitale e costi operativi, quali l'assunzione di consulenti di sicurezza e dei sistemi.

Anatomia di un attacco mirato

In teoria, le catene di attacco mirato sembrano abbastanza semplici: ricognizione e testing, penetration, propagazione, esecuzione, esito. Questo potrebbe suggerire che, bloccando automaticamente i primi passi di un attacco a più fasi, l'attacco in sé può essere sventato.



Gli attacchi mirati sono processi a lungo termine, che compromettono la sicurezza e forniscono al criminale controllo non autorizzato sull'infrastruttura IT della vittima. Questi attacchi consentono al criminale di non essere rilevato dalle tecnologie di sicurezza tradizionali.

Sebbene alcuni attacchi si servano di minacce avanzate persistenti (APT), molto efficienti ma costose, altri possono utilizzare una tecnica unica, come un malware avanzato o un attacco zero-day.

Ma in realtà, gli attacchi mirati sono altamente sofisticati e non lineari per quanto riguarda il loro stato di avanzamento e l'esecuzione. Le capacità di individuazione così automatizzate, il monitoraggio continuo e la ricerca di minacce si dovrebbero applicare come parte di una strategia di difesa a più fasi.

Un attacco mirato è un processo lungo che viola la sicurezza e consente a un cybercriminale di ignorare le procedure di autorizzazione e di interagire con l'infrastruttura IT, evitando in questo modo di essere individuato dai mezzi tradizionali.

Quindi, prima di tutto, è un processo, un'attività continua, un progetto piuttosto che un'azione dannosa una tantum. Secondo la nostra esperienza nel monitoraggio degli attacchi a livello globale, tali operazioni tendono a durare almeno 100 giorni e per le agenzie di governo, i grandi operatori del mercato e le infrastrutture critiche, il tempo può essere calcolato in anni.

In secondo luogo, il processo è destinato a una specifica infrastruttura, progettato per ovviare a specifici meccanismi di sicurezza e potrebbe anche comportare inizialmente una presa di mira nei confronti di determinati dipendenti attraverso e-mail o social media. Questo è un approccio completamente diverso dalle e-mail di massa degli ordinari software dannosi ad opera di aggressori, i quali perseguono obiettivi totalmente diversi. Nel caso di un attacco mirato, la metodologia e le fasi della catena criminale sono destinate ad una vittima specifica.

In terzo luogo, è di solito un gruppo organizzato o un team di professionisti, talvolta internazionali, a gestire questa operazione, provvisti di sofisticati strumenti tecnici. Si potrebbe dire che la loro attività non sia solo un progetto, bensì un'operazione di combattimento su più fronti. Per esempio, i pirati informatici, potrebbero compilare un elenco di dipendenti, così da sfruttarli come porta di accesso all'organizzazione, e studiare i loro profili online e l'attività sui social media, con l'obiettivo di prendere il controllo dei loro PC aziendali. Il computer dei dipendenti è infetto, pertanto gli invasori procedono, stabilendo il controllo della rete attraverso la quale possono dirigere le loro attività criminali.

Sfide per la sicurezza di impresa

Il rischio di minacce sofisticate sta crescendo in maniera esponenziale, per questo molte imprese hanno già implementato tecnologie e servizi nella speranza di raggiungere un buon livello di protezione. Tuttavia, senza un approccio poliedrico e di pianificazione strategica, tali sforzi possono andare al di sotto delle aspettative.

Risultati deludenti di "lacunosi" o non strutturati investimenti per la sicurezza possono includere:

1. Importanti investimenti in una sandbox, in tecnologie autonome o nella costruzione di un SOC: ognuno di questi potrebbe comunque non essere efficiente nel migliorare gli standard di cybersecurity.

Le tecniche di protezione del perimetro, tra cui firewall e software anti-malware, risultano sufficienti per tenere testa ad alcuni degli attacchi più opportunistici. Gli attacchi mirati sono tutta un'altra questione.

Alcuni fornitori hanno cercato di risolvere il problema tramite una serie di prodotti autonomi e separati: sandbox, strumenti di analisi delle anomalie sulla rete o addirittura il monitoraggio specifico degli endpoint. Sebbene tutti questi singoli elementi siano in grado di offrire, anche efficacemente, una certa protezione e di bloccare il kit di strumenti dei criminali, non sono sufficienti di per sé per rilevare un attacco mirato e coordinato.

Per raggiungere questo obiettivo, si richiede il rilevamento di numerosi eventi che si verificano su tutti i livelli dell'infrastruttura aziendale. Le informazioni ottenute possono quindi essere elaborate utilizzando un sistema di analisi multilivello, seguita da un'interpretazione che applica un'intelligence per la sicurezza in tempo reale, proveniente da fonte attendibile. In altre parole, il migliore investimento è un approccio che integri il meglio di molte tecnologie, compresa la sandbox con le analisi di anomalie sulla rete ed eventi sugli endpoint, in un processo completo.

2. Le attuali soluzioni generano un numero eccessivo di eventi correlati alla sicurezza per il team SOC al fine di elaborare, analizzare, classificare e rispondere entro un ragionevole lasso di tempo.

3. La mancanza di adeguate competenze sulla sicurezza relativa agli attuali livelli di sofisticazione delle minacce. Gli esperti di sicurezza potrebbero essere abili nel rilevamento di incidenti e nel risanamento rapido (golden image, creazione di una blacklist di URL/file e costruzione di alcune regole) ma non pienamente qualificati per implementare un processo completo di risposta (qualifiche dei livelli di rischio, esecuzione di analisi iniziale, indagine, contenimento, analisi dei dati forensi).

4. La mancanza di visibilità delle operazioni. Durante un attacco mirato, i criminali informatici possono facilmente sottrarsi alle tradizionali soluzioni di sicurezza utilizzando credenziali rubate e software legittimi, in modo da non mostrare apparenti violazioni del sistema.

Dal momento che gli autori degli attacchi fanno di tutto per nascondere le attività dannose, può essere molto difficile individuare un attacco per il team responsabile della sicurezza IT di un'azienda. Ciò vuol dire che i criminali possono continuare a causare danni per periodi estesi.

La verità è che il malware è responsabile solo del 40% delle violazioni. Come si è visto, gli autori delle minacce utilizzano svariate tecniche per accedere ai sistemi aziendali.
Anche quando viene utilizzato il malware, il 70-90% di esso è specifico per l'organizzazione in cui viene rilevato in (Verizon: Data Breach Investigation Report).

5. Difficoltà a comprendere quale competenza impiegare e sviluppare in azienda, quali attività di sicurezza esternalizzare e che cosa può essere affidato in sicurezza ai sistemi automatizzati.

Con la crescente gravità degli incidenti di sicurezza e il loro potenziale impatto sull'efficacia delle aziende a livello globale, una delle principali sfide è quella di schierare in campo una gamma di esperti adeguatamente qualificati. Una completa ed efficace strategia di protezione richiede non solo un continuo monitoraggio e individuazione delle capacità, ma una risposta rapida e un qualificato risanamento, con adeguati processi forensi a disposizione.

I team SOC convenzionali tendono a concentrarsi solo su una parte di questo obiettivo: rilevamento e risposta. L'implementazione di soluzioni automatizzate aiuta a liberare gli esperti dall'intraprendere i passi successivi nel processo di gestione degli incidenti, ma poche imprese sono pronte a mettere in pratica tutte le attività di alto livello al loro interno. Così la sfida è quella di identificare quali elementi del processo globale (gestione, qualificazione del rischio, organizzazione delle priorità, risanamento rapido) dovrebbero essere intrapresi dal team interno e quali (ricerca di malware, analisi forensi,risposta agli incidenti, rilevamento delle minacce) potrebbe essere esternalizzati, in maniera efficace, agli specialisti.

Una parola sulle sandbox

Molte delle "soluzioni per il rilevamento di attacchi mirati" disponibili sul mercato sono composte da una sola sandbox autonoma. Persino i fornitori che non hanno mai rilevato minacce nuove e avanzate affermano di offrire sandbox, che sono spesso poco più di un'estensione dei rispettivi motori anti-malware e che non sono supportate da una threat intelligence funzionale.

La sandbox avanzata di Kaspersky Lab è solo una parte aggiuntiva alle nostre capacità di rilevamento integrate. È stata sviluppata direttamente dal complesso sandbox in laboratorio, la tecnologia che usiamo da più di un decennio. Le sue capacità sono state perfezionate su informazioni statistiche raccolte da dieci anni di analisi delle minacce, rendendola matura e focalizzata.

Il SOC di impresa basato sull'intelligence

I cybercriminali hanno adattato le proprie tecniche per eludere le difese tradizionali e nascondersi indisturbati nei sistemi per mesi o addirittura anni. È tempo per la protezione aziendale di adattarsi a sua volta, considerando un approccio multilivello basato su intelligence ai fini della sicurezza IT.

Fino a poco tempo fa, per difendere il perimetro aziendale era sufficiente utilizzare le tecnologie di sicurezza comuni che prevenivano le infezioni da malware o l'accesso non autorizzato alla rete aziendale. Tuttavia, oggi, con l'aumento di attacchi mirati, questo semplice approccio non è più sufficiente.

Se il dipartimento di sicurezza ha intenzione di difendersi da nuovi pericoli, sarà necessario un approccio alla protezione altamente adattabile e poliedrico, basato su un convenzionale SOC, migliorato da threat intelligence e soluzioni multilivello per la sicurezza.

Miglioramento dei processi per la sicurezza dell'impresa

Il reparto di Information Security è responsabile della protezione organizzativa e tecnica di informazioni fondamentali e di processi aziendali, in ambienti IT spesso complessi. Questo include, per esempio, la crescente adozione di soluzioni automatizzate e componenti software e la transizione verso la gestione dei documenti elettronici.

La crescita smisurata del numero di minacce avanzate e attacchi mirati ha generato un numero sempre crescente di soluzioni. I processi esistenti devono essere aggiornati al fine di raccogliere, memorizzare ed elaborare i dati generati non strutturati e di identificare e dare priorità agli attacchi complessi e multilivello. Questi includono:

- la valutazione dei fattori potenzialmente indicativi di un possibile attacco mirato;
- la raccolta di informazioni circa gli attacchi mirati e minacce statisticamente avanzate;
- l'identificazione e la risposta agli incidenti;
- l'analisi degli oggetti sospetti nel traffico di rete e allegati delle e-mail;
- rilevamento di attività anomale/insolite all'interno della infrastruttura protetta.

Nelle grandi imprese si sta rispondendo alle odierne minacce avanzate muovendosi verso la gestione centralizzata della sicurezza, consolidando i dati provenienti da diverse soluzioni di sicurezza (attraverso la raccolta dei dati automatizzata e la correlazione degli eventi, SIEM) e unificando la propria presentazione mediante la costruzione di centri per il monitoraggio della sicurezza (SOC, Security Operations Center). Tuttavia, affinché questo approccio sia efficace contro gli attacchi mirati e le minacce avanzate, è necessaria una completa comprensione dei problemi di sicurezza e la profonda conoscenza dell'analisi delle minacce informatiche.

Soluzione Threat Management and Defense

Kaspersky Lab è stata la prima azienda nel settore tecnologico a istituire un laboratorio dedicato alle minacce avanzate nel 2008.

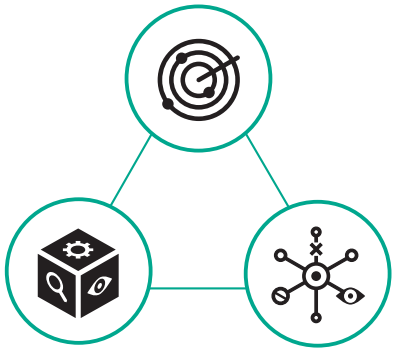
Quando si apprende la notizia che è stata rilevata una recente APT vi sono delle possibilità che ad individuarla sia stato il prestigioso team di ricerca globale e analisi di Kaspersky Lab, il team GReAT.

Con un invidiabile e comprovato successo nel rilevamento degli attacchi mirati e APT, il team GReAT è rinomato per la sua threat intelligence. Il team ha svolto un ruolo importante nella scoperta degli attacchi più sofisticati, tra cui:

- Stuxnet
- RedOctober
- Flame
- Miniduke
- Epic Turla
- DarkHotel
- Duqu
- Carbanak
- Equation

... e molti altri.

Kaspersky Anti Targeted Attack: protezione dalle minacce complesse



Kaspersky Cybersecurity Services: outsourcing e approfondimenti di sicurezza

Kaspersky Endpoint Detection and Response: visibilità completa

Kaspersky Lab, tramite lo studio del funzionamento interno di alcune delle minacce mondiali più sofisticate, hai sviluppato un portfolio di tecnologie e servizi strategici in grado di offrire un approccio alla sicurezza completamente integrato e adattivo. Grazie alla nostra competenza, Kaspersky Lab ha raggiunto i primi posti nelle classifiche dei test indipendenti sul rilevamento e sulla mitigazione delle minacce un numero di volte maggiore rispetto ad altre aziende del settore della sicurezza IT. Ora, abbiamo lavorato per assemblare le competenze sul rilevamento degli attacchi mirati in un'unica soluzione autonoma, risultato di due decenni di ricerca e analisi sulle minacce che hanno generato tecnologie mature e comprovate.

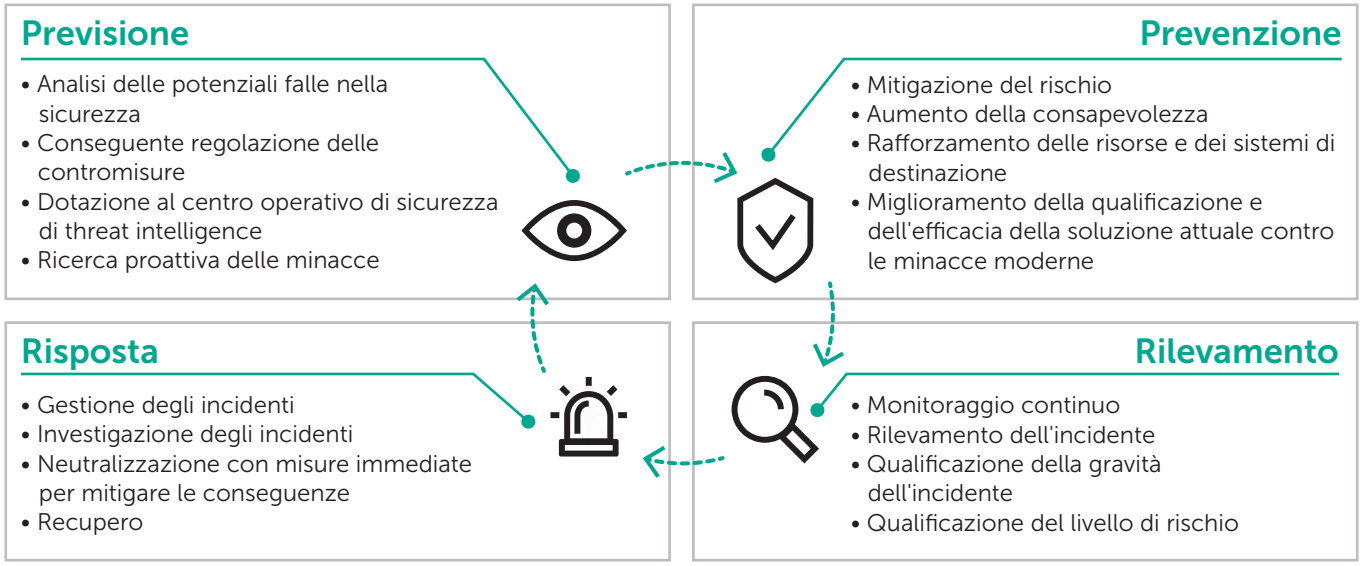
Sebbene la maggior parte delle minacce informatiche semplici possa essere bloccata da prodotti di sicurezza tradizionali ed euristici basati su firma, i cybercriminali e gli hacker oggi utilizzano un numero crescente di attacchi sofisticati per colpire organizzazioni specifiche. Gli attacchi mirati, tra cui le Avanced Persistent Threat (APT), rappresentano oggi uno dei rischi più pericolosi che le aziende si trovano ad affrontare. Tuttavia, mentre le minacce, e le tecniche impiegate da cybercriminali e hacker, sono in continua evoluzione, molte aziende non riescono ad adattare le proprie strategie per la sicurezza.

Combinando il rilevamento multilivello dalla piattaforma Kaspersky Anti Targeted Attack e la reazione rapida di Kaspersky Endpoint Detection e, ancora, la risposta con i servizi di intelligence di cybersecurity e assistenza premium, Kaspersky Threat Management and Defense fornisce una soluzione unificata, che consente di automatizzare e facilitare l'intero ciclo di gestione delle minacce avanzate.

Più difficili da rilevare e, spesso, più complicati da eliminare, gli attacchi mirati e le minacce avanzate richiedono una strategia di sicurezza adattiva e completa. La soluzione Kaspersky Threat Management and Defense è fondata sulla più fattibile architettura di sicurezza come descritto da Gartner. Il nostro approccio è quello di fornire un ciclo di attività in quattro aree chiave: prevenzione, rilevamento, risposta e previsione.

- **Prevenzione**: ridurre il rischio di minacce avanzate e attacchi mirati
- **Rilevamento**: individuare le attività che indicano un attacco mirato
- **Risposta**: sanare le falle di sicurezza e indagare sugli attacchi
- **Previsione**: dove e quando potrebbero verificarsi nuovi attacchi mirati

Essenzialmente, questo presuppone che i tradizionali sistemi di prevenzione funzionino in coordinamento con le tecnologie di rilevamento, con l'analisi delle minacce, con le capacità di risposta e con le tecniche predittive per la sicurezza. Questo aiuta a creare un sistema di cybersecurity che si adatta continuamente e risponde alle nuove sfide aziendali.

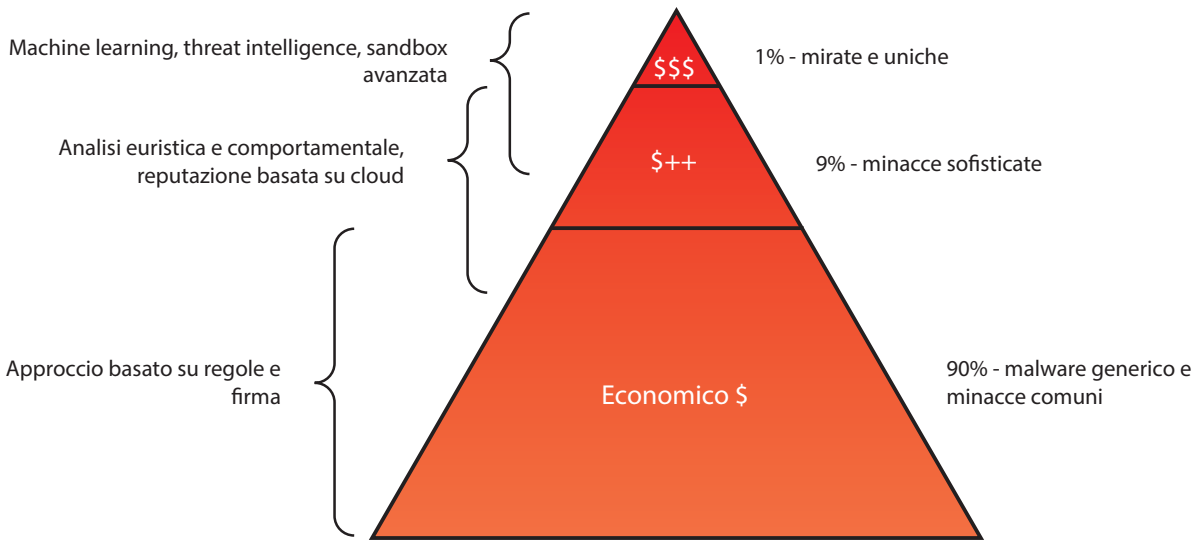


Prevenzione: uso delle pluripremiate tecnologie di sicurezza per ridurre il rischio di attacchi mirati

Per gli attacchi mirati, le tecnologie di prevenzione sono utili per filtrare gli incidenti irrilevanti, gli oggetti comuni dannosi e le comunicazioni inconsistenti.

La prevenzione, basata su prodotti di sicurezza, può essere molto efficace nella protezione contro le minacce comuni, tra cui il malware, attacchi di rete, fuga di dati e altro ancora. Tuttavia, anche queste tecnologie non sono sufficienti per proteggere un'azienda dagli attacchi mirati. Durante l'attacco, le tecnologie tradizionali per la sicurezza basate sulla prevenzione potrebbero rilevare alcuni incidenti, ma generalmente non sono in grado di stabilire se ogni singolo incidente è parte di un attacco più pericoloso e complesso che potrebbe causare gravi danni all'azienda e continuare a provocare danni per lunghi periodi.

Tuttavia, le tecnologie multilivello basate sulla prevenzione costituiscono un elemento chiave per il nuovo approccio proattivo che mira a difendere l'azienda dagli attacchi mirati.



Affrontare minacce diverse con tecnologie di sicurezza

L'80% degli attacchi mirati inizia con un messaggio e-mail dannoso, contenente un allegato o un link.

Gli obiettivi preferiti di infiltrazione dei cybercriminali includono: le risorse umane, i call center, gli assistenti personali dell'alta dirigenza e le aree esternalizzate dell'azienda. Queste sono considerate come le aree meno preparate dell'organizzazione.

È essenziale per le organizzazioni aziendali continuare ad usare le tecnologie "tradizionali" per:

1. automatizzare il filtro e il blocco degli eventi e degli incidenti non correlati ad attacchi mirati, che contribuirà a evitare inutili distrazioni per la scoperta di incidenti pertinenti;

2. rafforzare l'infrastruttura IT contro tecniche economiche e facili da eseguire (social engineering, dispositivi rimovibili, dispositivi mobili, malware e recapito e-mail dannoso ecc.). Infatti tutti i precedenti investimenti sul perimetro e la sicurezza degli endpoint, insieme ai controlli implementati, contribuiscono ad aumentare la quantità di sforzo e di investimenti richiesti dai cybercriminali al fine di penetrare nella rete.

Ma se il pirata informatico è altamente motivato e, forse, persino ingaggiato da una terza parte per condurre con successo un attacco, non sarà sufficiente una prevenzione basata su un unico approccio.

Rilevamento: individuazione di più vettori di minacce avanzate prima che si verifichi il danno

La Piattaforma Kaspersky Anti Targeted Attack comprende:

- **architettura multilivello a sensori** per una visibilità completa. Attraverso una combinazione di rete, Web, e-mail e sensori di endpoint, KATA fornisce rilevamento avanzato ad ogni livello dell'infrastruttura IT aziendale;
- **sandbox avanzata** per la valutazione delle nuove minacce. La nostra Sandbox avanzata, risultato di più di dieci anni di continuo sviluppo, offre un ambiente virtualizzato isolato, dove è possibile eseguire gli oggetti sospetti in maniera sicura e osservarne il comportamento;
- **motori di analisi potenti** per risposte rapide e un numero ridotto di falsi positivi. Il nostro strumento per l'analisi degli attacchi mirati verifica i dati provenienti dalla rete e dai sensori endpoint e genera velocemente il rapporto sul rilevamento della minaccia per il team responsabile della sicurezza aziendale.

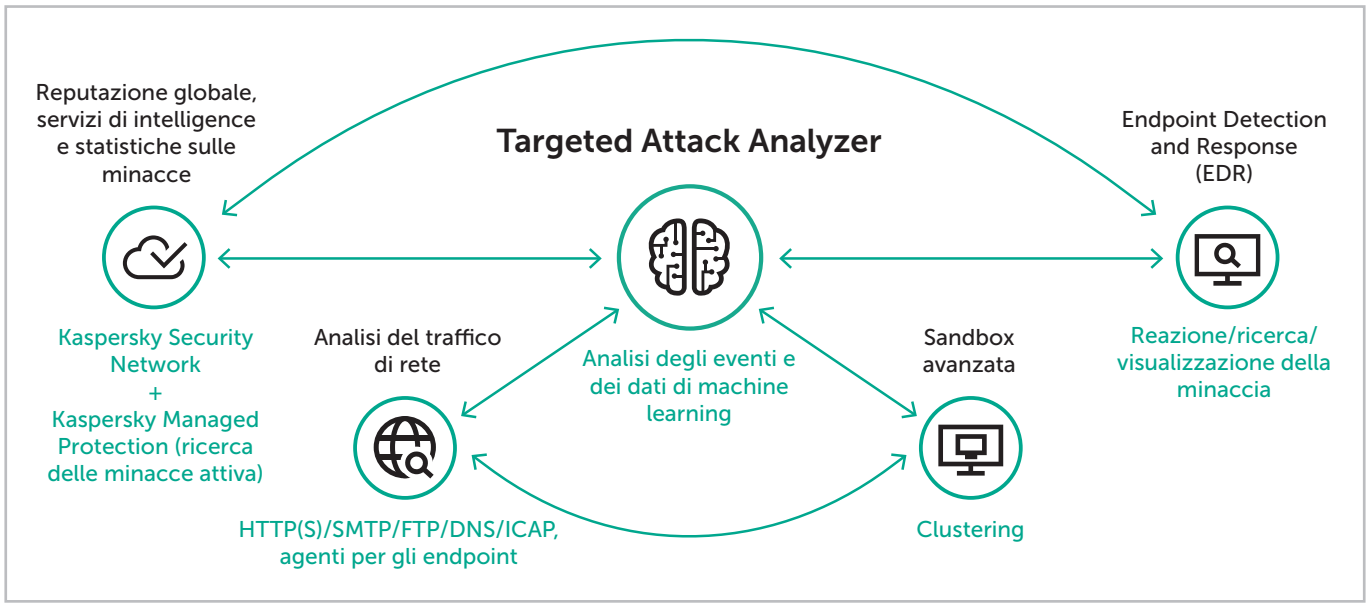
Prima si rileva l'attacco, minori saranno le perdite finanziarie e l'organizzazione patirà una minore interruzione. Pertanto, la qualità e l'efficacia di rilevamento è di fondamentale importanza.

Dal momento che gli attacchi mirati sono composti e complessi, il rilevamento implica una solida competenza pratica sul funzionamento degli attacchi avanzati e mirati. Le soluzioni anti-malware semplici non sono in grado di difendere l'azienda da questi tipi di attacco. Sono invece necessarie tecnologie di rilevamento con accesso a dati di threat intelligence più recentemente aggiornati, in grado di eseguire analisi dettagliate dei comportamenti sospetti che potrebbero verificarsi sui diversi livelli della rete aziendale.

La capacità di rilevare gli attacchi mirati è formata da soluzioni connesse e servizi in grado di offrire:

- Formazione
- **Esperienza del rilevamento dell'attacco mirato**: controllare una volta sola l'infrastruttura per trovare tracce di compromissione;
- **Soluzione specializzata**: piattaforma Kaspersky Anti Targeted Attack + Kaspersky Endpoint Detection and Response;
- **Feed di dati sulle minacce** per uno scambio e un aggiornamento in tempo reale sulle nuove minacce;
- **Report APT e personalizzati** per una migliore comprensione delle fonti e dei metodi della minaccia
- **Rilevamento delle minacce 24 ore su 24, 7 giorni su 7** Kaspersky Managed Protection Service.

Basata sui principali strumenti di sicurezza e tecnologie avanzate di machine learning, nella piattaforma Kaspersky Anti Targeted Attack si combinano dati endpoint e di rete, sandbox e intelligence analysis per correlare gli incidenti, cercare indicatori di compromissione e aiutare a rilevare gli attacchi mirati più complessi. Il collegamento dei vari elementi di un incidente fornisce una vista completa di tutta la catena di attacco, aumentando la fiducia nella percentuale netta di minacce assegnata e riducendo i falsi positivi a zero.

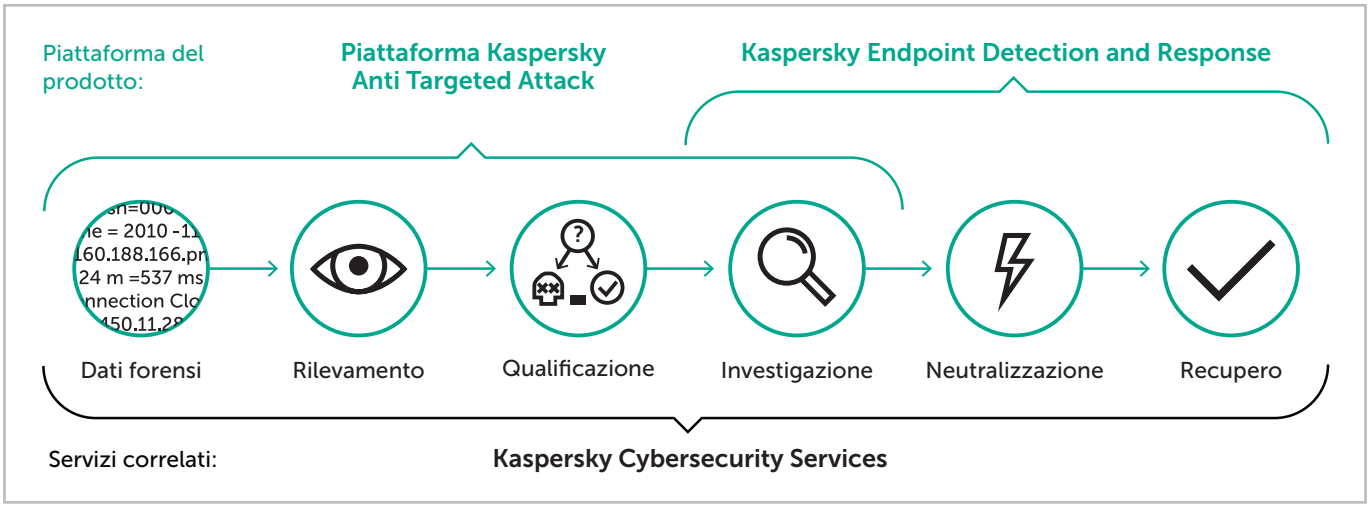


La risposta, cioè come aiutare le aziende a riprendersi da un attacco

Ovviamente, raggiungere un tasso di rilevamento elevato è solo una parte della battaglia. Le migliori tecnologie di rilevamento non si sfruttano abbastanza se non si dispone di strumenti e delle competenze necessarie per rispondere rapidamente alla minaccia "in tempo reale" che sta danneggiando potenzialmente l'organizzazione

Dopo il rilevamento di un attacco, è importante consultare esperti di sicurezza riconosciuti, dotati delle competenze e dell'esperienza adatte ad aiutare a:

- valutare e correggere il danno;
- ripristinare rapidamente le operazioni;
- pianificare azioni per prevenire un'ulteriore ripetizione dello scenario del medesimo attacco.



Kaspersky Endpoint Detection and Response offre:

- **Rilevamento avanzato**: grazie al Machine Learning,Targeted Attack Analyzer (TAA), crea una linea di base di comportamento degli endpoint. Questo consente di abilitare un record storico che si può utilizzare per scoprire il modo in cui si è verificata una violazione.
- **Threat Hunting proattivo** grazie alla ricerca rapida, utilizzando un database centralizzato, insieme alla ricerca di indicatori di compromissione (IoC) per supportare attivamente il team di cybersecurity, scansionando gli endpoint in modo proattivo per individuare eventuali anomalie e violazioni della sicurezza.
- **Adaptive Threat Response** che include una vasta gamma di risposte automatiche che aiutano le imprese a evitare l'uso di tradizionali processi di correzione, come la cancellazione e la ricreazione immagine, che può causare costosi tempi di inattività e perdita di produttività.

Una volta che la piattaforma Kaspersky Anti Targeted Attack identifica l'attacco, entra in campo Kaspersky Endpoint Detection and Response. È il successivo componente vitale della Threat Management and Defense solution, che consente alle aziende di accelerare il processo di risposta agli incidenti e di migliorare la qualità dell'inchiesta degli incidenti di cybersecurity.

Kaspersky EDR fornisce la gestione centralizzata degli incidenti su tutti gli endpoint della rete aziendale, garantendo un flusso di lavoro senza interruzioni e un'integrazione con il rilevamento di rete tramite la piattaforma Kaspersky Anti Targeted Attack. Una vasta gamma di risposte automatizzate aiuta a evitare i costosi tempi di inattività e perdita di produttività intrinsechi nei tradizionali processi di correzione, come la cancellazione e la ricreazione di immagine. Mediante il monitoraggio e il controllo di una vasta gamma di funzioni da una singola interfaccia, le attività di sicurezza possono essere eseguite in modo più efficiente ed efficace, senza dover saltare tra più strumenti e console.

Visibilità completa e accurata rilevazione sono solo una parte della battaglia. La natura stessa degli attacchi mirati è che i loro autori prima o poi ritorneranno con nuovi strumenti e nuove tecniche. Se si verifica un'emergenza, il team per la cybersecurity potrebbe aver bisogno di un partner fidato con competenze ed esperienza rilevanti, così come di perfezionare le competenze aziendali.

Il nostro servizio di risposta agli incidenti comprende:

- **Valutazione dell'incidente.** Analisi iniziale dell'incidente con risultati rapidi, per aiutare a ridurre al minimo i danni all'azienda (l'analisi può essere eseguita in loco o da remoto)

- **Raccolta delle prove.** Ad esempio, raccolta delle immagini del disco rigido, dati estratti dalla memoria, tracce sulla rete e altre informazioni relative all'incidente

- **Analisi forense.** Analisi dettagliate per acquisire informazioni come:
  - che cosa è stato aggredito;
  - chi ha perpetrato l'attacco;
  - il periodo in cui l'azienda ha subito l'attacco;
  - dove ha avuto origine l'attacco;
  - perché l'azienda è stata attaccata;
  - in che modo è stato implementato l'attacco.

- **Analisi del malware.** Analisi dettagliata del malware utilizzato come parte dell'attacco.

- **Piano di correzione.** Un piano dettagliato per aiutare l'azienda a prevenire la propagazione del malware sul resto della rete e la creazione di un piano di disinstallazione.

- **Report sulle indagini.** Un report dettagliato che comprende informazioni relative alle indagini condotte sull'incidente e alle possibili modalità di correzione.

Anche se il team responsabile della sicurezza della vostra azienda è in grado di portare a termine molte attività di risposta all'incidente, potreste decidere di usufruire di altri servizi offerti da Kaspersky:

- **Servizio di analisi del malware**: preleva il malware isolato dal team interno per sottoporlo ad analisi dettagliata.

- **Servizio di analisi forense digitale**: analisi delle prove digitali e degli effetti dell'incidente riscontrati dal proprio team.

Previsione: agire per difendersi dalle minacce future

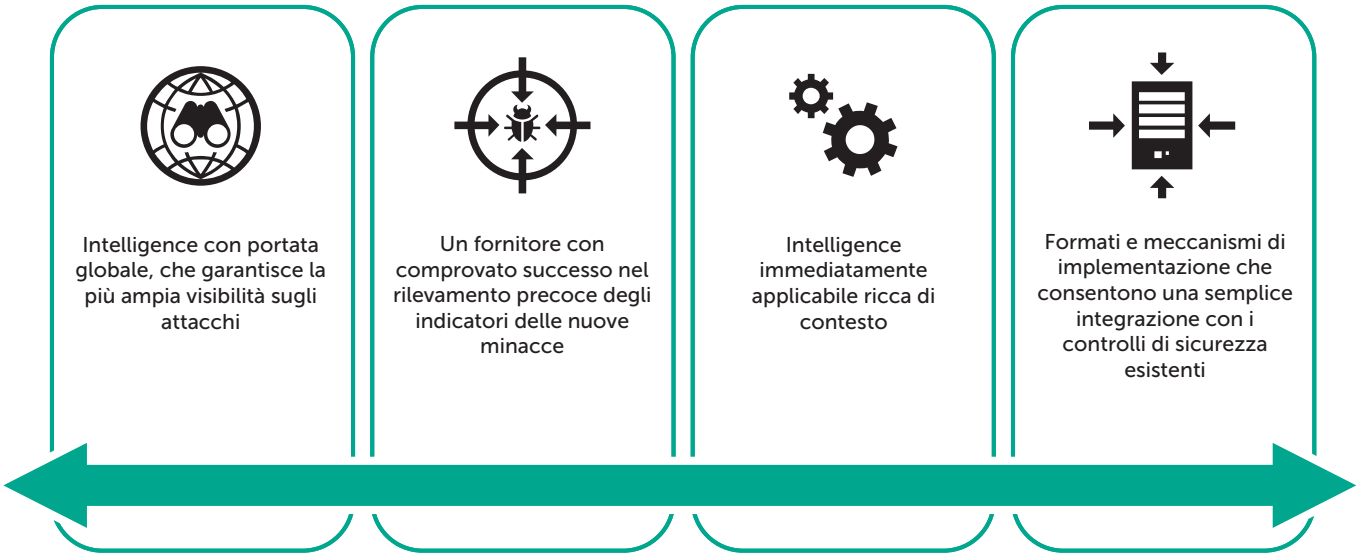
Con la costante evoluzione del panorama delle minacce, la strategia di sicurezza deve adattarsi continuamente alle nuove sfide.

La sicurezza non è un'attività "una tantum", ma un processo continuo che richiede la valutazione regolare di:

- minacce più recenti;
- efficienza della propria sicurezza IT.

... per consentire all'azienda di adattarsi ai nuovi rischi e ai cambiamenti.

Accesso alla threat intelligence globale con Kaspersky Lab



È pertanto molto importante consultare esperti che possano tenervi aggiornati sul panorama globale delle minacce e aiutarvi a testare i sistemi e le difese in uso al fine di aiutare l'organizzazione ad adattarsi e a stare al passo con le nuove minacce alla sicurezza.

Nel corso degli anni, gli esperti di sicurezza globale hanno acquisito un'ampia quantità di conoscenze sul funzionamento degli attacchi avanzati e degli attacchi mirati e si continuano ad analizzare costantemente le nuove tecniche di attacco. Questa "sudata" esperienza si traduce in una posizione privilegiata per la previsione di nuovi metodi d'attacco e aiuta a prepararsi a combatterli.

Inoltre, offriamo servizi specializzati per rafforzare l'infrastruttura IT della vostra azienda:

- Servizi di penetration test: un aiuto per la valutazione dell'efficienza delle dotazioni attuali per la sicurezza
- Servizi di valutazione della sicurezza delle applicazioni: per il rilevamento delle vulnerabilità dei software, prima che vengano scoperte dai cybercriminali
- Formazione avanzata sulla cybersecurity: per formare gli esperti interni all'azienda e per creare il proprio Centro operativo di sicurezza
- Report sulla threat intelligence e report personalizzati sulle minacce: per mantenere l'aggiornato sul panorama moderno delle minacce, in continua evoluzione
- Portale Threat Lookup: accesso al database d'intelligence globale di Kaspersky Lab per supportare il potenziamento delle ricerche del malware

La strategia di sicurezza adattativa di Kaspersky è fondata sulla più fattibile architettura di sicurezza come descritto da Gartner. L'approccio di Kaspersky Lab fornisce un ciclo di attività in quattro aree chiave: prevenzione, rilevamento, risposta e previsione. In sostanza, si assume che i tradizionali sistemi di prevenzione dovrebbero funzionare in collegamento con le tecnologie di rilevamento, con l'analisi delle minacce, con le capacità di risposta e con le tecniche predittive per la sicurezza. Questo aiuta a creare un sistema di cybersecurity che si adatta continuamente e risponde alle nuove sfide aziendali.

L'adozione della soluzione Kaspersky Lab's Threat Management and Defense significa:

1. Spostarsi da un modello reattivo per la sicurezza a un modello proattivo basato sulla gestione del rischio, sul monitoraggio continuo, su una risposta agli incidenti più informata e su capacità di rilevamento delle minacce.

2. Nella framework si semplifica il processo di protezione e si aumenta l'efficacia della sicurezza mediante un modello di difesa multistrato in cui si impedisce e si rileva la presenza di minacce avanzate in ogni fase di attacco.

3. In una piattaforma integrata si riducono gli avvisi di sicurezza che gravano sulla maggior parte dei team per la sicurezza, fornendo un contesto basato sulla threat intelligence e priorità per gli avvisi, nonché per migliorare le risposte tattiche attraverso la condivisione della conoscenza delle minacce, di una approfondita competenza e fornendo servizi di intelligence per la sicurezza.

4. Questo ambiente fornisce analisti della sicurezza con visibilità di tutte le fasi di attacco in modo unificato, consentendo una perfetta analisi delle minacce e un'inchiesta affidabile sia delle minacce note sia di quelle sconosciute, prima del loro impatto sulle attività aziendali.

5. La condivisione della Threat Intelligence globale, fornisce insights proattive specifiche rispetto alle motivazioni e alle intenzioni dei propri avversari, in modo che sia possibile definire, di conseguenza, le priorità dei criteri e la pianificazione degli investimenti di sicurezza.

Tecnologie Kaspersky Lab: un mondo di esperienza

Nel 2017 i prodotti Kaspersky Lab hanno partecipato a 86 test e recensioni indipendenti. I nostri prodotti hanno vinto per 72 volte il primo premio e per 78 volte sono rientrati nei primi tre posti. Le metriche TOP3 rappresentano i punteggi aggregati ottenuti da oltre 80 noti fornitori nelle recensioni e nei test indipendenti più rispettati del settore della sicurezza. Le prestazioni sostenute tra più test e prodotti garantiscono una valutazione notevolmente superiore rispetto alla valutazione una tantum delle prestazioni sulla base di un solo test.

Soluzione comprovata contro le minacce avanzate

Nel 2017, vi è stata una continuità di partecipazione ai test ICSA Lab della piattaforma Kaspersky Anti-Targeted Attack (come parte della soluzione Threat Management and Defense).

Gli ultimi test hanno avuto la durata di 37 giorni e consistevano in 585 attacchi e 519 file puliti. KATA ha ottenuto risultati eccellenti:

- perfetto tasso di rilevamento: 100% (zero campioni persi);
- il più basso tasso possibile di falsi positivi: 0%;
- raggiungimento dello status "Certified".

Di seguito, vi sono alcune citazioni del report ICSA il 7 luglio:

- "La soluzione Kaspersky è stata notevole durante questo ciclo di prova".
- "La piattaforma KATA di Kaspersky Lab ha rilevato il 100,0% delle minacce incontrate durante il test, un risultato di gran lunga migliore rispetto alla percentuale necessaria per la certificazione".
- "Kaspersky Labs' KATA ha dimostrato un'eccellente efficacia nell'individuazione delle minacce, contro quasi 600 nuovi e poco conosciuti pericoli".
- "Indipendentemente da quanto sia nuova o vecchia la minaccia, la piattaforma KATA di Kaspersky ha rilevato tutte le nuove e poco conosciute minacce dannose".
- "La piattaforma KATA di Kaspersky ha avuto zero falsi positivi durante questo ciclo di prova, un eccellente risultato".
- "La soluzione di difesa dalle minacce avanzate KATA di Kaspersky Labs ha superato tutti i test per mantenere la ICSA Labs Advanced Threat Defense Certification. Il completamento di questo ciclo di prova segna il 3° trimestre consecutivo per Kaspersky Lab di soddisfazione dei criteri di certificazione ICSA Labs ATD".

NOTA: la metodologia dei test ICSA è dinamica e cambia da un trimestre all'altro. Il test è di per sé una continua simulazione di un ambiente reale e di metodi di attacco. Non si misura il livello di protezione in un dato momento, ma per un periodo di tempo esteso (più di trenta giorni) di funzionamento continuo sotto numerosi attacchi. In questo modo, nella prova si dimostra l'efficienza e l'efficacia di una soluzione dal punto di vista dell'utente.

Approccio visionario e completo

Per diversi anni Radicati Group ha condotto un'analisi indipendente del mercato per le soluzioni di protezione APT, rivelando i principali operatori, i Trail Blazer, gli specialisti e gli operatori maturi. Nel risultato delle analisi di mercato, appena rilasciato, si è valutato in maniera eccellente l'approccio di Kaspersky Lab, che consiste nel contare gli attacchi mirati e le minacce avanzate.

Nel 2017, la soluzione Kaspersky ha migliorato significativamente la sua posizione con un maggiore spostamento dagli specialisti ai leder di Trail Blazering.

I fornitori di Trail Blazing offrono le migliori tecnologie avanzate, in alcune aree delle loro soluzioni, ma non necessariamente hanno tutte le caratteristiche e funzionalità che li classificherebbero come migliori operatori. I Trail Blazer, tuttavia, hanno il potenziale per "interrompere" il mercato con nuove tecnologie o nuovi modelli di erogazione. Col passare del tempo, è più probabile che questi fornitori diventino migliori operatori.

"La piattaforma Kaspersky Anti Targeted Attack fornisce il rilevamento delle minacce avanzate e degli attacchi mirati in tutti i livelli di un attacco: infezione iniziale, comunicazioni command and control, movimenti laterali ed estrazione dei dati".

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Novità sulle minacce informatiche: **www.securelist.com**
Novità sulla sicurezza IT: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.it