kaspersky bring on the future

Come proteggere le organizzazioni da cyberattacchi complessi

Siete mai rimasti svegli la notte per la preoccupazione che qualche minaccia informatica avanzata potesse annidarsi nell'infrastruttura della vostra azienda, in attesa del momento giusto per rubare la proprietà intellettuale o tenere in ostaggio la vostra organizzazione?

Se è capitato anche a voi, fate bene a preoccuparvi. Come suggerisce il nome, le minacce APT (Advanced Persistent Threat) ricorrono a sofisticate tecniche di hacking per ottenere l'accesso ai vostri sistemi. Una volta che violano le vostre difese, possono agire indisturbate per mesi o addirittura anni, ottenendo privilegi di accesso di livello superiore e raccogliendo ed esfiltrando i dati con risultati potenzialmente devastanti.

Chi è a rischio?

Come prevedibile, mettere a punto un attacco APT o mirato richiede una quantità significativa di competenze, impegno e risorse, con il risultato che gli obiettivi primari solitamente sono i settori governativi o le grandi organizzazioni con dati sensibili o proprietari che giustificano l'investimento.

Ciò nonostante, le minacce APT sono un metodo di attacco che dovrebbe destare la preoccupazione delle aziende di tutto il mondo, dal momento che anche le imprese di medie dimensioni sono potenzialmente a rischio.

Gli autori di attacchi APT, ad esempio, stanno prendendo sempre più di mira le aziende più piccole che fanno parte delle supply chain dei loro obiettivi finali. Dal momento che le aziende di questo tipo di solito sono meno sicure, possono essere utilizzate come trampolino di lancio verso le organizzazioni più grandi con cui lavorano.

Per questo motivo, sia che la vostra azienda sia un'importante organizzazione o un'impresa più piccola potenzialmente sfruttabile per prendere di mira un'organizzazione più grande, è importante **comprendere la natura delle minacce** con cui potreste avere a che fare. Stiamo parlando delle minacce APT e di altri attacchi mirati, ma anche delle capacità richieste per difendervi da questi pericoli.

Tutti i settori interessati

Negli ultimi due anni, gli attacchi mirati human-driven si sono verificati in tutti i settori. Nel 2024, i settori IT e della Pubblica Amministrazione sono stati in testa con il 14,7% e il 13,8%, rispettivamente.

Fonte: Kaspersky Managed Detection and Response 2024 Analyst Report

4.88 milioni di dollari

Costo medio globale di un data breach nel 2024, con un aumento del 10% rispetto al 2023 e il totale più alto mai registrato. Nell'area del Medio Oriente, questo indicatore è notevolmente più elevato e raggiunge gli 8,75 milioni di dollari.

Fonte: Rapporto di IBM sul costo di un data breach nel 2024

258 giorni

Tempo necessario per identificare e contenere una violazione. Questo periodo di recupero esteso non solo inasprisce le perdite finanziarie, ma lascia anche le organizzazioni vulnerabili a ulteriori attacchi.

Fonte: Rapporto di IBM sul costo di un data breach nel 2024

Come funzionano le minacce APT?

L'idea alla base di una minaccia APT è ottenere un accesso permanente o continuativo ai sistemi IT e/o OT (Operational Technology) dell'obiettivo, che di solito gli hacker ottengono attraverso un processo in cinque fasi.

Figura 1: fasi di una minaccia APT in evoluzione

Fase 1

Ottenere l'accesso

Come un ladro che forza una porta con un piede di porco, spesso i cybercriminali ottengono l'accesso inizialmente utilizzando un "piede di porco digitale", come un file infetto, posta elettronica indesiderata o messaggi di phishing oppure una vulnerabilità in un'applicazione, per inserire malware nella rete interessata.

Fase 2

Stabilire un punto di appoggio

Così facendo, installano malware che consente loro di creare backdoor e tunnel che possono usare per spostarsi nei sistemi senza essere individuati.

Fase 3

Accedere a livelli più profondi

Una volta entrati nella rete, gli hacker utilizzano tecniche quali la violazione delle password per ottenere i diritti di amministratore, in modo da poter controllare una parte maggiore del sistema e raggiungere livelli di accesso ancora superiori.

Fase 4

Spostarsi lateralmente

Arrivati più in profondità all'interno del sistema e in possesso degli stessi diritti dell'amministratore di rete, possono muoversi come vogliono. In questo modo, possono accedere a più server e ad altre parti sicure della rete.

Fase 5

Guardare, imparare e rimanere

Con un accesso più in profondità al sistema, i cybercriminali riescono a capire pienamente come funziona l'ambiente, a conoscere le sue vulnerabilità e a raccogliere tutte le informazioni che vogliono. Possono anche tentare di mantenere questo processo in atto, potenzialmente all'infinito, o ritirarsi dopo aver raggiunto il loro obiettivo.

Quali sono le potenziali conseguenze di un attacco APT?

Basta leggere le esperienze riportate da una qualunque organizzazione che abbia subito un attacco mirato per comprendere chiaramente che gli effetti possono essere gravi e duraturi. Se le ripercussioni immediate possono includere normalmente danni finanziari causati dalla perdita di dati e dall'interruzione delle attività, gli effetti più a lungo termine possono comprendere danni alla reputazione dell'organizzazione, perdita di fiducia dei clienti e potenziali azioni legali.

A questo, naturalmente, si aggiunge il problema di rimediare ai danni all'infrastruttura IT dell'organizzazione, processo che spesso richiede mesi o talvolta anche anni per giungere a termine. E a seconda del settore in cui opera la vostra azienda, possono esserci anche conseguenze specifiche per il settore in questione.

Figura 2: analisi dell'impatto delle minacce APT sulla sicurezza aziendale

Finanza

- Interruzioni dei servizi critici
- Transazioni non autorizzate
- Attacchi cash-out
- Conseguenze legali del furto di identità

Amministrazioni

- Potenziali effetti del cyberspionaggio
- Danni all'infrastruttura critica
- Discontinuità dei servizi di e-government
- Esposizione dei dati personali dei cittadini

E-commerce

- Implicazioni legali del furto di account tramite furto di identità
- Transazioni fraudolente
- Negazione dei servizi IT, perdita di profitti
- Potenziali sanzioni ai sensi di GDPR, PCI DSS, ecc.

Trasporti

- Discontinuità e arresti delle operazioni
- Ritardi nella supply chain e aumento dei costi
- Minaccia alla vita
- Danni all'infrastruttura critica

Alimentare

- Carenza di scorte e arresti della produzione
- Compromissione della qualità degli alimenti
- Potenziale contaminazione con sostanze chimiche, tossine, ecc.
- Necessità di ripiegare sulle operazioni manuali

Sanità

- Interruzioni dei servizi critici
- Esposizione dei dati personali dei pazienti
- Fiducia del pubblico minata
- Potenziale minaccia alla vita

IT e telecomunicazioni

- Perdita di clienti
- Perdita nelle vendite
- Interruzioni di rete non pianificate
- Interruzioni del servizio sui dispositivi mobili o fissi

Industria

- Disastri ambientali
- Discontinuità delle operazioni
- Maggiori interruzioni non pianificate del servizio
- Guasti a cascata o blackout a livello di sistema

>2

incidenti di criticità elevata accadono ogni giorno.

43%

di tutti gli incidenti di criticità elevata rilevati da Kaspersky nel 2024 è rappresentato da attacchi mirati human-driven (APT).

Fonte: Kaspersky Managed Detection and Response 2024 Analyst Report

Cosa comporta per le difese informatiche dell'azienda?

Uno dei pericoli principali delle minacce APT e di altri attacchi mirati è che anche se vengono scoperti e la minaccia immediata sembra essere svanita, gli hacker possono avere lasciato più backdoor, per poter tornare quando vogliono.

Un altro problema è che molte difese informatiche tradizionali, come gli antivirus e i firewall, di solito non forniscono protezione contro questo tipo di attacchi.

Dal breve riepilogo sopra riportato delle fasi per la creazione di un attacco APT o mirato, dovrebbe apparire evidente che per difendersi da queste minacce serve un approccio multilivello, che includa soluzioni in grado di proteggere endpoint, reti, cloud, e-mail, accesso a Internet e molto altro.

Questo non solo contribuirà a prevenire e diminuire il rischio di attacchi sofisticati, ma aiuterà anche a ridurre al minimo l'interruzione delle attività e i costi legati a questo tipo di incidenti, qualora dovessero verificarsi.

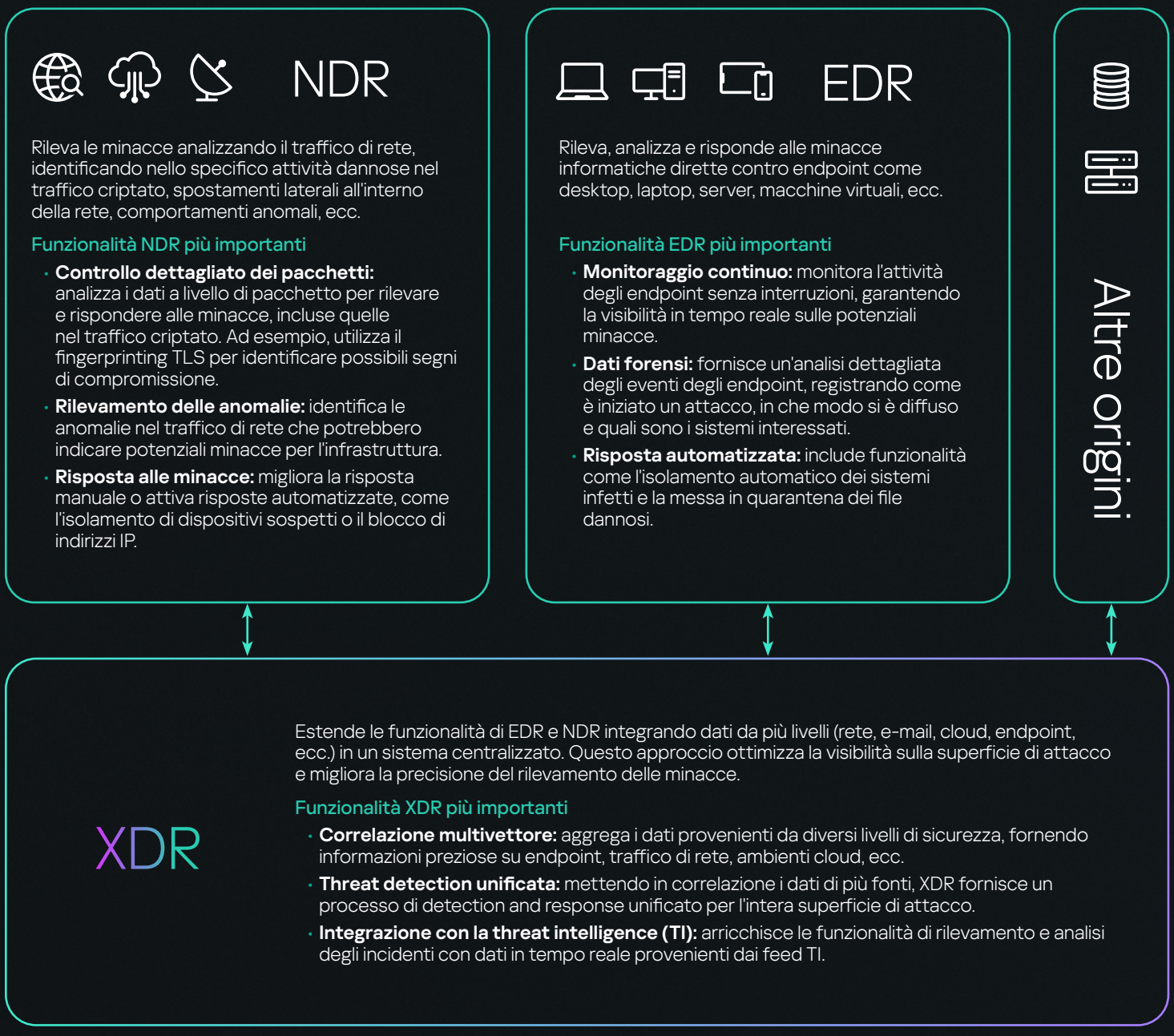
Quindi, quali sono le possibili soluzioni e in che modo dovreste implementarle?

Come proteggere le organizzazioni da cyberattacchi complessi

Se una piattaforma EPP (Endpoint Protection Platform) di per sé non assicura protezione contro gli attacchi mirati, fornirà comunque un'origine dati essenziale da utilizzare nell'analisi di attacchi nuovi, in corso o passati. Di conseguenza, dovrebbe essere usata come parte di una gamma di soluzioni che include anche:

- Endpoint Detection and Response (EDR) – Offre protezione degli endpoint e visibilità a livello di dispositivo, identifica e risponde alle minacce su workstation, server, ecc.
- Network Detection and Response (NDR) – Monitora e analizza il traffico di rete, rileva le anomalie e risponde alle potenziali minacce a livello di rete.
- Extended Detection and Response (XDR) – Integra EDR, NDR e altri livelli di sicurezza per ottimizzare la visibilità e automatizzare la risposta alle minacce.

Figura 3: EDR, NDR, XDR: come funzionano?



Nel 2024, il tempo medio per indagare e segnalare incidenti di criticità elevata è aumentato del 48%, indicando un incremento della complessità media degli attacchi rispetto al 2023. Ciò è supportato dal fatto che la maggior parte delle regole di rilevamento attivate e degli IoA proveniva da strumenti XDR specializzati, anziché dai log del sistema operativo come negli anni precedenti.

Fonte: Kaspersky Managed Detection and Response 2024 Analyst Report

Quindi quale soluzione scegliere?

La scelta della giusta soluzione, o della giusta combinazione di soluzioni, dipende dalle esigenze specifiche dell'organizzazione, oltre che dall'infrastruttura e dal panorama delle minacce:

- Scegliete EDR se gli strumenti di protezione degli endpoint tradizionali non sono più sufficienti e avete bisogno di una protezione più avanzata contro le minacce informatiche (come malware, ransomware, phishing e altro ancora).
- Scegliete NDR se le minacce basate sulla rete sono la vostra principale preoccupazione e avete bisogno di funzionalità avanzate per analizzare e rispondere alle anomalie nel traffico di rete.
- Scegliete XDR se desiderate una protezione completa su più vettori e volete essere in grado di correlare le minacce all'interno dell'intera infrastruttura IT.
- Ancora meglio, combinate EDR, NDR e XDR in un unico ecosistema di sicurezza per garantire una difesa completa contro una vasta gamma di minacce informatiche avanzate ed elusive.

Figura 4: EDR, NDR, XDR: per chi sono più adatte?

Soluzione di cybersecurity	Per quale organizzazione è più adatta?
EDR	• Organizzazioni che danno la priorità alla protezione degli endpoint e hanno bisogno in informazioni dettagliate in tempo reale sull'attività degli endpoint. • Organizzazioni con molti endpoint distribuiti, come istituzioni finanziarie o fornitori di servizi sanitari, che potranno trarre il massimo vantaggio dalla capacità di EDR di rilevare e rispondere in tempo reale alle minacce basate sugli endpoint.
NDR	• Organizzazioni che fanno molto affidamento sul traffico di rete e hanno bisogno di capacità avanzate per il rilevamento di minacce basate sulla rete. • Aziende con un team di sicurezza IT dedicato o organizzazioni altamente regolamentate come datacenter, provider di servizi o enti governativi, che possono beneficiare della capacità di NDR di rilevare e rispondere alle minacce basate sulla rete.
XDR	• Organizzazioni che necessitano di una piattaforma di sicurezza unificata con funzionalità complete di rilevamento e risposta alle minacce all'interno dell'intera infrastruttura IT. • Grandi organizzazioni con ambienti IT complessi che hanno bisogno di un approccio completo alla sicurezza. Ad esempio, una società multinazionale con datacenter on-premises e ambienti cloud potrebbe trarre vantaggio dalla capacità di XDR di fornire il rilevamento delle minacce unificato tra più piattaforme, riducendo al tempo stesso la complessità operativa grazie alla centralizzazione dell'incident response.

Kaspersky Anti Targeted Attack

Il contributo di Kaspersky

Kaspersky Anti Targeted Attack (KATA) assicura una protezione completa anti-APT contro informatiche più complesse. Aiuta le organizzazioni a:

- Rilevare, analizzare e rispondere rapidamente agli attacchi mirati.
- Garantire una solida protezione su tutti i principali punti di ingresso degli attacchi, inclusi reti, e-mail, Web ed endpoint.
- Salvaguardare le risorse critiche.
- Assicurare la conformità alle normative del settore.

Questo è reso possibile dall'utilizzo delle potenti tecnologie NDR e EDR disponibili nei tre livelli di Kaspersky Anti Targeted Attack.

I tre livelli di KATA offrono protezione contro le minacce APT (Advanced Persistent Threat) sfruttando le funzionalità essenziali così come quelle avanzate di NDR, fino a quelle XDR native.

- KATA: funge da soluzione NDR essenziale e offre funzionalità di base per rilevare e rispondere alle minacce informatiche.
- KATA NDR Enhanced: basato sulle funzionalità fondamentali del livello KATA, offre capacità NDR avanzate.
- KATA Ultra: combina capacità NDR e EDR per fornire funzionalità XDR native. Protegge i molteplici punti di ingresso delle minacce, tra cui reti, Web, e-mail, endpoint, server e macchine virtuali.

Figura 5: Kaspersky Anti Targeted Attack. Una scelta flessibile.

Criteri di confronto	KATA	KATA NDR Enhanced	KATA Ultra
Descrizione	Essential NDR	NDR avanzate	NDR+EDR (XDR nativo)
Funzionalità NDR essenziali	•	•	•
Sandbox avanzata	•	•	•
Integrazione di Kaspersky Threat Intelligence e MITRE ATT&CK	•	•	•
Funzionalità NDR avanzata		•	•
Funzionalità EDR per esperti			•
Funzionalità XDR native			•

Scegliete tra le funzionalità NDR del livello Essential o Advanced oppure optate per la soluzione combinata NDR+EDR per gli scenari XDR nativi, per proteggere la vostra azienda dalle minacce informatiche più sofisticate, il tutto da un'unica piattaforma. Al livello KATA Ultra, otterrete una protezione completa all-in-one contro le minacce APT e una visibilità sull'intera infrastruttura IT.

Perché scegliere Kaspersky Anti Targeted Attack

Visibilità completa sulla vostra infrastruttura IT

Offre un set completo di tecnologie uniche per eliminare i punti ciechi e avere sotto controllo tutti i potenziali punti di accesso delle minacce, inclusi rete, Web, endpoint ed e-mail, il tutto da una singola piattaforma unificata.

Protezione supportata dalla threat intelligence globale

Arricchisce l'analisi e la risposta alle minacce tramite l'accesso diretto al database di reputazione globale di Kaspersky Private Security Network, a Kaspersky Threat Intelligence e alla mappatura sul framework MITRE ATT&CK.

Tecnologie comprovate e testate in modo indipendente

Utilizza tecnologie innovative per il rilevamento delle minacce avanzato basato su machine learning, indagini approfondite e incident response rapido, la cui affidabilità è riconosciuta dalle più importanti agenzie di analisi e dai principali clienti in tutto il mondo.

Kaspersky Anti-Targeted Attack

Per saperne di più

Presentazione video di Kaspersky Anti Targeted Attack

Guardate

Previsioni delle minacce avanzate

Leggete ora

www.kaspersky.it